Appendix G: Program Requirements for Development of a Rail Transit Agency System Security and Emergency Preparedness Program Plan (SEPP)

SAMPLE

State Oversight Agency Program Requirements for the Development of Rail Transit System Security and Emergency Preparedness Plans

This document has been developed to serve as a template for use by state oversight agencies in specifying the requirements established in 49 CFR Part 659 for the development of a rail transit agency System Security and Emergency Preparedness Plan (SEPP). It includes a sample set of Program Requirements, detailing the required SEPP contents and a set of recommended SEPP appendices.

Table of Contents

SEPP Memorandum of Executive Approval/System Security Policy

- ***Element:*** *A policy statement should be developed for the System Security and Emergency Preparedness Plan.*

In this section, a policy statement should be provided which establishes the System Security and Emergency Preparedness Plan (SEPP) as an operating document that has been prepared for, and approved by, rail transit agency top management.

- ***Element:*** *The policy statement should describe the authority that establishes the SEPP, including statutory requirements and the rail transit agency's relationship with the oversight agency.*

The policy statement should define, as clearly as possible, the authority for the establishment and implementation of the SEPP. As appropriate, reference should be made to the authority provided by state and local statues to develop and securely operate the rail transit system and coordinate with local, state and federal agencies regarding security and emergency preparedness issues. The role of the SEPP in addressing FTA's 49 CFR Part 659 and state oversight agency requirements should be clearly described. Participation in programs managed by the Department of Homeland Security, Office of Grants and Training (G&T) (formerly the Office of State and Local Government Coordination and Preparedness (SLGCP), Office for Domestic Preparedness (ODP)) and the Transportation Security Administration (TSA) that require the SEPP should also be mentioned, including the Transit Security Grant Program (TSGP) and compliance with TSA directives and the TSA Rail Security Inspector Program.

- ***Element:*** *The policy statement is signed and endorsed by the rail transit agency's chief executive.*

Reference should be made to management's approval, either by referencing the enabling signature on the title page or by other means.

1. System Security and Emergency Preparedness Program Introduction

1.1. PURPOSE OF THE SEPP

- ***Element:*** *The SEPP should identify the purpose of the security program endorsed by the agency's chief executive.*

This section of the SEPP should identify its purpose. For most rail transit agencies, the purpose of the SEPP is to ensure a planned, documented, organized response to actual and potential security threats to the system, and to address these threats with proactive measures and response techniques that manage and minimize the outcome of security breaches or related events. The SEPP typically:

- develops, documents, and communicates a comprehensive, responsive, appropriate and effective security and emergency preparedness program;

- documents security and emergency preparedness goals and objectives for the rail transit agency, as official direction to employees and department managers, and as a performance accountability basis for the agency's security program;
- serves as the rail transit agency's in-house point-of-reference for a complete and comprehensive description of its security and emergency preparedness program;
- fulfills regulations promulgated by FTA ("Rail Fixed Guideway Systems; State Safety Oversight" (49 CFR Part 659)) and the state oversight agency (cite state regulations) to address the security of passengers and employees and to ensure their protection from emergencies, including terrorism and natural disasters;
- supports rail transit agency compliance with region-wide initiatives to address requirements specified in Homeland Security Presidential Directives (HSPDs) for the National Response Plan, the National Incident Management System the National Infrastructure Protection Plan, and the National Response Goal;
- fulfills DHS/G&T requirements for Transit Security Grant Program (TSGP) assistance; and
- ensures compliance with TSA directives, including RAILPAX-04-01 issued on May 20, 2004.

As set forth in rail transit agency's security program policy, accountability for security and emergency preparedness of the rail transit system rests with each employee, supervisor, manager, director, and department. As a result of this program, the rail transit agency will achieve not only an effective physical security program, but also develop emergency preparedness.

The rail transit agency's plans for response to natural disaster or terrorism incidents are based on partnerships with the emergency management and first-responder organizations of the cities and counties throughout the rail transit agency's service area, and the region's coordinated plans for response and recovery from such events. This coordination is essential for the rail transit agency's response and recovery capabilities, while at the same time, continuity of rail transit operations during a community-wide emergency is a vital capability for the region's recovery.

1.1.1 System Security

- ***Element:*** *The SEPP should introduce the concept of "system security."*

System security is defined as:

"the application of operating, technical, and management techniques and principles to the security aspects of a system throughout its life to reduce threats and vulnerabilities to the most practical level through the most effective use of available resources."

System security provides a structured methodology for analyzing threats and weighing the consequences of the cost of their resolution against the capabilities of the system to fund improvements. This process allows the system; whatever its size, service, or operating environment; to implement the most effective security and preparedness program possible within its available resources. System security promotes an integrated approach to protection, identifying

how all system activities come together as part of an interdependent system that deters, detects, assesses, and responds to threats.

1.1.2 Emergency Preparedness

- ***Element:*** *The SEPP introduce the concept of "emergency preparedness."*

Within the context of this approach, emergency preparedness is a central feature of the program, ensuring the capability to mitigate and manage those events that cannot be prevented. Emergency preparedness is defined as:

"a uniform basis for operating policies and procedures for mobilizing public transportation system and other public safety resources to assure rapid, controlled, and predictable responses to various types of transportation and community emergencies."

Emergency preparedness ensures that the rail transit agency has a process in place to provide fast, controlled and predictable responses to various types of emergencies that may occur within the system or nearby locations. Emergency preparedness identifies how municipal and county agencies can both support, and obtain support from, the rail transit agency in addressing transit-specific and area-wide emergencies.

1.2 GOALS AND OBJECTIVES

1.2.1 Goals

- ***Element****: The SEPP should identify the goals of the SEPP program endorsed by the agency's chief executive.*

This section of the SEPP should identify the goals developed by the rail transit agency to meet the purpose established for the SEPP. Goals are broad statements of ideal future conditions for the safety program that are desired by the rail transit agency, endorsed by top management, and are supported by specific objectives to aid in their attainment. Goals should be realistic and generally are presented in qualitative terms.

Sample goals include the following:

1. **Security**: Reduce the rate of crime, and the fear of crime, on the rail transit system.

2. **Awareness and Involvement**: Engage all rail transit employees and contractor personnel in a program of awareness activities to ensure that they serve as "eyes and ears" for the system. Also establish a similar process of engagement in awareness activities for passengers and others who come into contact with the system.

3. **System Approach**: Systematically and continually identify, assess and resolve threats to the security of the system, optimizing use of human resources, operating procedures, technology and equipment, facilities design and improvements, and community and interagency partnerships, to maximize security effectiveness.

4. **Emergency Preparedness**: Develop and implement **P**lans, **O**rganization, **E**quipment, **T**raining/procedures, and emergency **E**xercises/evaluation (POETE) to assure preparedness for catastrophic natural disasters or terrorist attacks. These POETE activities should be appropriately coordinated and integrated with the emergency management/response jurisdictions in the rail transit agency's service area, and should support compliance with Homeland Security Presidential Directives (HSPDs) requiring implementation of the National Response Plan (NRP), the National Incident Management System (NIMS), the National Infrastructure Protection Plan (NIPP), and the National Preparedness Goal. The rail transit agency's activities to support implementation of HSPD requirements may be coordinated through the Regional Transit Security Working Group (RTSWG) and the Regional Transit Security Strategy (RTSS).

1.2.2 Objectives

- ***Element****: The SEPP should identify the objectives of the SEPP program endorsed by the agency's chief executive.*

Objectives are the working elements of the SEPP, the means by which the identified goals are achieved. Unlike goals, objectives should be easily quantifiable. They should provide a framework for guiding the day-to-day activities that provide for a safe and secure rail transit operation. Objectives are often supported by the identification of associated tasks that are required to be completed. Objectives for the sample goals identified above are presented in the table on the next page.

GOALS AND OBJECTIVES	
Goal #1. Security: Reduce the rate of crime, and the fear of crime, on the rail transit system.	
Objective 1.A	Maintain 100,000 boarding rides or better per reported crime on the rail transit system, as measured by crimes occurring on the system reported to police.
Objective 1.B	Maintain 70% or better customer rating of "good" or "excellent" addressing concerns about security on board the rail system, as measured through the rail transit agency's annual Attitude and Awareness survey.
Objective 1.C	Maintain 300,000 or better boarding rides per customer complaint about security or vandalism, as measured through rail transit agency's Customer Service Information (CSI) system.
Goal # 2. Awareness and Involvement: Engage all rail transit employees and contractor personnel in a program of awareness activities to ensure that they serve as "eyes and ears" for the system. Also establish a similar process of engagement in awareness activities for passengers and others who come into contact with the system.	
Objective 2.A	Achieve broad-based awareness of security responsibilities, alertness and procedures by rail transit personnel (means of measurement to be determined).
Objective 2.B	Achieve broad-based security alertness by rail transit agency customers (means of measurement to be determined).
Goal # 3. System Approach: Systematically and continually identify, assess and resolve threats to the security of the system, optimizing use of human resources, operating procedures, technology and equipment, facilities design and improvements, and community and interagency partnerships, to maximize security effectiveness.	
Objective 3.A	Systematically determine and assess deployments and tactics of dedicated security personnel, in relation to systematically analyzed information on crime, threats, and effectiveness on customer perception of security on the transit system.
Objective 3.B	Continually foster partnerships with law enforcement jurisdictions and community organizations, in support and extension of the rail transit agency's dedicated security resources.
Objective 3.C.	Systematically incorporate security design considerations and security technology and equipment into design of rail transit agency facilities.
Goal # 4. Emergency Preparedness: Develop and implement **P**lans, **O**rganization, **E**quipment, **T**raining/procedures, and emergency **E**xercises/evaluation (POETE) for preparedness to perform the prevention, detection, response and recovery capabilities applicable to rail transit systems and their employees during catastrophic natural disasters or terrorist attacks. These activities should be appropriately integrated with emergency management/public safety jurisdictions in the rail transit agency's service area, and should support compliance with Homeland Security Presidential Directives (HSPDs) requiring implementation of the National Response Plan (NRP), the National Incident Management System (NIMS), the National Infrastructure Protection Plan (NIPP), and the National Preparedness Goal. The rail transit agency's activities to support implementation of HSPD requirements will be coordinated through the Regional Transit Security Working Group (RTSWG) and the Regional Transit Security Strategy (RTSS).	
Objective 4.A	Develop and implement the rail transit agency's internal emergency preparedness POETE through integration of these activities into the agency's Emergency Operations Plan and into the development of Memorandum of Understanding (MOUs) with external agencies.
Objective 4.B	Develop and implement the rail transit agency's external emergency preparedness, through the development of procedures, training and emergency exercises, by partnering with the emergency management and first-responder organizations of cities and counties throughout the rail transit agency's service area, to integrate POETE needed for natural disaster or terrorism incidents on the transit system, and into the region's coordinated, mutual POETE for response and recovery from such events.

1.3 SCOPE OF PROGRAM

- ***Element**: Describe the scope of the SEPP and Program.*

This section of the SEPP should establish the scope of the SEPP to cover all agency personnel, and be applicable to all agency operations:

- each department/function shall support the rail transit agency's SEPP and shall cooperate in achievement of the SEPP security objectives;
- each rail transit agency employee shall cooperate with the system safety and security/police functions and provide them with any information requested to aid in any threat or vulnerability identification, assessment or resolution, and/or security investigation; and
- accountability for security and emergency preparedness of the rail transit system rests with each employee, supervisor, manager, director.

The Scope should also specify that coordinating and integrating the emergency response plans of the rail transit agency and of the jurisdictions in the agency's service area, is part of the SEPP program.

1.4 SECURITY AND LAW ENFORCEMENT

- ***Element**: Describe the security and law enforcement functions that manage and support implementation of the SEPP.*

This section of the SEPP should describe the security and law enforcement functions that manage and support implementation of the SEPP. If the rail transit agency has its own police force, this section of the SEPP should introduce this department and provide an overview of the department's activities. Also, this section of the SEPP should identify the rail transit police responsibilities regarding relationships with other law enforcement agencies in the municipalities traversed by the rail transit system.

If the rail transit system purchases security services from local law enforcement agency(s), the plan should introduce this arrangement, and provide an overview of the mechanisms in place to integrate contracted law enforcement services into the rail transit agency's day-to-day operations. This section of the SEPP should also clarify which function within the rail transit agency manages this contract, and how activities are coordinated with other law enforcement agencies in the rail transit agency's service area.

If the system employs its own security (non-sworn) force or purchases security services from a private company, the plan should provide an overview of these security forces and identify the methodologies used to support cooperation with local law enforcement agencies in the rail transit agency's service area. This section of the SEPP should also clarify which function within the rail transit agency manages this contract or in-house security force.

If the system depends solely on local law enforcement for primary response, the plan should discuss how the system interacts with local law enforcement and what formal or informal arrangements or agreements, including any memorandum of understanding (MOU), are in place. If the system uses any combination of these types of security configurations, the SEPP should provide an overview of how the various components of the security/police function work together.

Whatever the rail transit operator's police or security configuration, the SEPP should explain how staff officers work with, communicate with, coordinate activities with, and share jurisdiction with local law enforcement agencies. In this discussion, the rail transit agency should include information regarding response to incidents, planning and deployment, joint operations, special events, and the sharing the threat and crime information.

1.5 MANAGEMENT AUTHORITY AND LEGAL ASPECTS

- ***Element**: Describe the authority which oversees the operation and management of the rail transit agency, including its security/police function.*

This section of the SEPP should describe the authority which oversees the operation and management of the rail transit agency, including its security/police function. The section should identify the charter or legislation which created the rail transit agency, and address the roles of the Board of Directors, General Manager, other executive leadership, and the manager of the security/police function in executing the SEPP. Municipal, county and state codes that are enforced on the transit system should be identified, including ordinances for fare evasion, parking enforcement, vandalism, disorderly conduct, and other public order violations. Any special authorities provided to transit police, contracted law enforcement, contracted private security or in-house security personnel should also be identified.

In preparing this section, the rail transit agency may first introduce its charter, enabling legislation and/or cooperative agreements with the municipalities and counties in its service area. Then, after describing the role of the Board of Directors (providing stewardship and budget approval for the transit agency) and the General Manager (approves and issues the SEPP, established policy that assigns responsibility for developing, implementing and administering the SEPP), this section may identify the roles of other management positions (Executive Director, Operations; Director of Safety and Security, Chief of Police/Security Manager) and explain how each is responsible for developing and enforcing the Standard Operating Procedures (SOPs), operating orders, training, rules compliance programs, evaluation programs, internal security audits, and other activities that assure implementation of the SEPP.

Then, the roles and responsibilities of middle management and line personnel may be briefly introduced and described (i.e., management within the transit security/police function, as well as the roles of supervisors and operations and maintenance personnel). Finally, the section may conclude with a discussion of the ordinances, codes, rules and other laws enforced on the rail transit system (i.e., felonies and misdemeanors applicable to the transit agency's service area, fare evasion, vandalism, unlawful entry (trespass) upon transit property or vehicles, interference with movement of or access to transit vehicles, disorderly conduct on transit property or in transit vehicles, and offensive physical contact with a transit passenger, employee, agent, security officer or police officer).

This section of the SEPP should provide a high-level overview only. SEPP management and implementation will be discussed in greater detail in Chapters 3 and 4.

1.6 GOVERNMENT INVOLVEMENT

- ***Element**: Describe how the SEPP interfaces with local, state and federal authorities to ensure security and emergency preparedness for the system.*

This section of the SEPP should introduce and briefly describe the local, state and federal agencies with whom the rail transit agency coordinates for security and emergency preparedness. For example, at the federal level, the rail transit agency may coordinate with government agencies for funding support and to ensure compliance with security regulations and grant requirements. Federal partners may include: FTA, Federal Highway Administration (FHWA), Federal Railroad Administration (FRA), DHS, and its subsidiary bureaus, including G&T, the Federal Emergency Management Agency (FEMA), and TSA.

In working with FTA, 49 USC 5307(J)(i) requires that a recipient of federal transportation funds under 49 USCS 5336 spend at least one percent of the amount received on mass transportation security projects. The rail transit agency may consistently exceed the 1% utilization the FTA guideline.

In working with DHS, the rail transit agency may participate in the Transit Security Grant Program (TSGP), which is funded by G&T, and administered by the State Administrative Agency (SAA) and the regional Urban Area Security Initiative (UASI) Point-of-Contact Working Group (UAPOC). Participation in the TSGP requires the development of this SEPP, the implementation of an on-going threat and vulnerability assessment process, and creation of Regional Transit Security Working Groups (RTSWG) to develop and implement a Regional Transit Security Strategy (RTSS), in coordination with the SAA and UAPOC. G&T also offers technical assistance programs for establishing the RTSS, conducting rail transit threat and vulnerability assessment, and developing and conducting emergency exercises and evaluation.

The rail agency also coordinates with local, regional and state emergency management and public safety agencies to address other DHS requirements for implementation of the National Response Plan, the National Incident Management System, and the National Infrastructure Protection Plan. The rail transit agency may also support the TSA Rail Security Inspector Program, as well as research and pilot projects being performed by TSA, and ensure compliance with TSA directives. Appendix A provides additional information on these DHS, G&T and TSA programs.

State government coordination may include the state Department of Transportation (DOT), the state Office of Homeland Security, and the state SAA for the G&T TSGP program. The state oversight agency should also be discussed here, including its role in requiring, receiving, reviewing and approving the SEPP. *If the state oversight agency does not have protections in place to shield security documents from public release, then the procedures developed to review and approve these documents, discussed in Section 6 of this SEPP, should be briefly mentioned.* The state oversight agency's enabling legislation and/or program requirements may be referenced here or included as an appendix.

At the regional level, the rail transit agency may coordinate with the region's emergency management group, the county emergency management agency, or a county emergency management committee; the UAPOC; the local office of the Federal Bureau of Investigation's (FBI) Joint Terrorism Task Force (JTTF), and for transportation project funding, the region's Metropolitan Planning Organization (MPO). In supporting regional coordination, the rail transit agency may have signed intergovernmental agreements or memorandum of understanding (MOUs) to formally partner with the county/regional emergency management agency or committee, including requirements for participation in emergency management planning monthly coordination meetings and implementation of regional incident management and response protocols. The rail transit agency may have also joined the region's UASI working group, UAPOC, in support of the region's UASI Strategy, through implementation of the RTSS.

The rail transit agency may also have signed MOUs with local law enforcement, emergency medical services (EMS), fire departments, hospitals, and other transit providers in the region to address a range of issues associated with SEPP implementation.

1.7 Security Acronyms and Definitions

- ***Element****: Provide a listing of acronyms and definitions used in the SEPP.*

This section of the SEPP should include all of the acronyms and definitions used in the plan. Acronyms and definitions may be presented in this section or included in an Appendix that is referenced in this section. Appendices B and C of this document include sample acronym and definition lists.

2.0 System Description

The primary purpose of Chapter 2 is to provide organizational information and operating parameters for both those outside the organizations that need to understand the transit system, and those inside the organization to have clearly defined lines of report and responsibility delineation. The information presented should be sufficient to allow non-technical and non-transit persons to understand the system and its basic operations.

2.1 Background & History of System

- ***Element:*** *A description of the agency including general overview, a brief history and scope of rail transit services provided.*

This section should briefly describe the system's characteristics. This section should describe when and how the transit system was established, history of service delivery, major milestones in the transit system's history, and the modes of service provided. A system map and reference to the transit agency's website should also be provided.

2.2 ORGANIZATIONAL STRUCTURE

- ***Element:*** *Organizational charts showing the lines of authority and responsibility as they relate to security and emergency preparedness.*

This section of the SEPP should provide or reference:

- Detailed organizational diagrams for the rail transit agency showing the title of each position.
- Detailed diagram of the structure of the security/police function identifying the key positions at all levels.
- Diagrams showing the relationship and lines of communications between the security/police function and other units of the organization.
- The relationship of the transit system to local political jurisdictions, including law enforcement and emergency management agencies.

2.3 HUMAN RESOURCES

- ***Element:*** *Provide a categorization and break-down of all employees and contractors who work for/on the rail transit agency.*

This section of the SEPP should identify all departments supported at the rail transit agency and clarify how many full-time employees, part-time employees, and contracted personnel support them. For example, a table such as the one appearing below may be used.

Department	Full-time Employees	Part-Time Employees	Contractors
General and Administrative			
Capital Projects and Facilities			
CP&F Bus and Rail Facilities Management			
Operations			
Administration and Planning			
Safety and Security Department			
Director and Administrative Staff			
Security Staff			
Safety Staff			
Transit Police Officers			
Transit Security Officers			
Rider Advocates			
Deputy District Attorney			
Bus and Rail Transportation			
Transportation Staff and Supervisory			
Full-Time Bus Operators			
Part-Time Bus Operators			
Rail Operators			
Contracted Support			
Field Operations			
Field Operations Staff and Lead Supervisors			
Bus Dispatchers and Rail Controllers			
Bus and Rail Field Operations Supervisors			
Fare Inspection Field Operations Supervisors			
Accessible Transportation Programs			
Administrative and IT Staff			
Vehicle Operators			
Vehicle Maintainers			
Dispatchers			
Bus Maintenance			
Maintenance Staff and Supervisory			
Mechanics, Helpers, Cleaners, Clerks, Storekeepers			
Rail Maintenance (excl. Rail Facilities Management)			
Maintenance Staff and Supervisory			
Mechanics, Cleaners, Clerks, Storekeepers			

2.4 PASSENGERS

- ***Element:*** *Provide a description of the rail transit agency's ridership.*

This section of the SEPP should provide annual ridership statistics for the most recent year they are available. Ridership may be broken down mode of service and by day of week. Weekly and annual totals should also be provided. Major changes in ridership (increases, decreases, new service areas or expanded modes of service) should also be identified. Relevant statistics or information on system riders may also be included, such as: growth in population in service area, characteristics of typical riders (i.e., commuters, students, etc.), percentage of adults living in

service are who ride the system at least once a month, and information on the usage of accessible services and paratransit service.

2.5 SERVICES AND OPERATIONS

- ***Element:*** *Describe the rail transit agency's operations and services.*

In this section of the SEPP, the rail transit agency should provide information on the size, location, and function of the transit agency's physical assets including; maintenance facilities, offices, stations, vehicles, signals, and structures for all modes. This information, for each mode of service, may include: hours of operation, the number of vehicles, the number of routes, number of vehicles typically in peak and off-peak service, frequency of vehicles, the types of facilities owned and operated by the system and the types of activities performed there, and the names and addresses of relevant locations.

2.6 OPERATING ENVIRONMENT

- ***Element:*** *Describe the rail transit agency's operating environment.*

This section of the SEPP should describe the rail transit agency's operating environment, including traffic conditions, rail alignment, weather, issues associated with special events or other activities, safety issues associated with the rail transit service, and levels of crime in the communities served by the rail transit agency.

2.7 INTEGRATION WITH OTHER PLANS AND PROGRAMS

- ***Element:*** *Describe how the SEPP integrates with other plans and programs maintained by the rail transit agency.*

This section of the SEPP should discuss how the SEPP is integrated with the *System Safety Program Plan*, the *System Safety and Security Certification Program Plan*, the *Emergency Operations Plan*, *Incident Specific Response Plans*, *Facility Emergency/Evacuation Plans*, and other documents and programs that affect security and emergency preparedness, including the *Regional Transit Security Strategy*. A brief description of each of these documents should be provided, as well as the management interface which ensures coordination at the rail transit agency.

For example, the rail transit agency may state that the System Safety Program Plan and the SEPP are companion documents, and both are in accordance with FTA regulations concerning safety and security of transit systems, as implement by the state oversight agency. The rail transit agency may also specify that the Emergency Operations Plan and supporting training, drills and exercises are critical elements which support and reinforce SEPP provisions and procedures. Finally, the rail transit agency may identify how the SEPP supports, and is supported by, the *Regional Transit Security Strategy*, including the identification of tasks and G&T grant allocations to support achievement of SEPP goals and objectives.

2.8 CURRENT SECURITY CONDITIONS

- ***Element:*** *Description of the current security conditions at the rail transit agency and the types of security incidents experienced by the transit system and their frequency of occurrence*.

This section should describe current security conditions and issues at the transit agency including the incidents of crime experienced on the system and relevant information on passenger fear/perceptions of security. Crime data should be provided, documenting the most recent year for which it is available. The types of security incidents (including Part I and Part II offenses and ordinance violations) and their frequency of occurrence on the transit system should be included. Also this section should provide context for this information, including a comparison of crime rates at the transit system over time and/or a comparison of crime rates from the rail transit agency with crime rates for the municipalities in its service area.

2.9 CAPABILITIES AND PRACTICES

- ***Element:*** *Summary description of methods and procedures, devices, and systems utilized to prevent or minimize security breaches, including passenger education, campaigns, delay, detection, and assessment devices, and others that may be applicable.*

This section should summarize methods and procedures, devices, and systems utilized by the transit agency to minimize security incidents throughout the transit system. In addition, this section should also address activities performed to reduce passenger fear. This section should <u>not</u> provide detailed information on the security/police function or distinct security roles and responsibilities of specific elements of the rail transit organization (this information will be provided in Chapter 3). Instead, this section is intended to provide a broad overview of the types of activities performed by the rail transit agency to address the security conditions described in Section 2.8. In preparing this section, the rail transit agency may want to consider the following types of descriptions:

- **Theft and Vandalism at Park and Ride Lots, Transit Centers and Rail Transit Stations** -- Use of fixed-post and roving foot patrols, patrolling for suspicious persons at the parking facilities, using undercover surveillance in parked vehicles or camera-based enforcement to identify either suspicious vehicles or "at risk" vehicles, community crime prevention programs, trend analysis of crime data and customer service information, and joint operations with local law enforcement.
- **Drug Dealing at Rail Transit Stations/Facilities --** Continuing security patrols, undercover surveillance, and apprehension missions to control "open air" drug dealing, use of K-9 teams to support patrol and make arrests, bicycle patrol for heightened visibility and apprehension capabilities, partnership with local law enforcement and neighborhood associations, outreach in schools and coordination with community crime prevention programs.
- **Fare Evasion --** Use of fare inspectors with closely monitored fare enforcement goals, CCTV surveillance of fare vending machines and turnstiles, law enforcement "ride alongs" and vehicle boardings, steep fines and even arrests for violators, use of "no proof of purchase" as basis of policing/patrolling action (field identification cards,

warrant checks, etc.), outreach in schools and coordination with community crime prevention programs.

- **Rowdiness and Disruptive Behavior** -- Coordination with schools and the deployment of additional personnel during school-dismissal hours, targeted patrols and missions, in collaboration with local police agencies, strict enforcement of laws, local ordinances, and the rail transit agency's Code of Conduct, field identification and warrant checks, trend analysis on specific locations, and coordination and planning for special events.

Other Security Programs may be in place to address a range of passenger security issues and concerns, including:

- **Transit Passenger Waiting Zones** -- Located to ensure that evening and late-night riders can wait in a well-lit area with CCTV surveillance, emergency call boxes, and roving foot patrols, and then board the train in the first car, near the operator's compartment.
- **Radio Help Program** -- Rail transit operators can radio the rail Operations Control Center for help if someone needs emergency assistance, as part of the Radio Help Network. "Radio Help" decals are displayed on all transit vehicles.
- **Reward Program** -- The rail transit agency's Security Hotline may offer rewards of up to $1,000 for information leading to the arrest and conviction of a person(s) who assaults a rail transit operator/employee or vandalizes rail transit property.

Security-related features of the rail transit agency's vehicles, facilities and communication systems include the following:

- **Vehicles** -- Vehicles are equipped with on-board CCTV systems. Additional security features include: radio system for voice communication between Operators and Operations Control Center; enclosed, locked operator cabs on rail transit vehicles, passenger emergency intercoms to Operators on rail transit vehicles, "Be Alert" and "Transit Watch" notifications posted in all rail transit vehicles, to encourage passenger security awareness.
- **Operations Facilities and Offices** -- Internal security procedures at the rail transit agency require that doors providing access into facilities from outside are secured by the agency's card-key access control system or manually locked, except that doors providing public access may be unlocked during hours when staffed with reception/door monitoring personnel. Such personnel sign-in un-badged visitors and provide temporary, limited access cards. Key-locked doors and gates into security-sensitive areas use non-duplicatible keys, which are issued and tracked under a standard operating procedure (SOP). Operations facilities with vehicle or maintenance yards are secured with perimeter fencing, and by employee vigilance per agency SOPs to observe and question un-badged persons on the premises, and report the situation to the Operations Control Center if the person does not belong. Operating activities at operations facility locations are around-the-clock, all days. Following September 2001, the rail transit agency designated one or more on-site security representatives for each operations and office facility. Facilities received security assessments performed by the

agency's security/police function. A program of site-specific projects to strengthen internal facilities security was implemented in 2002. Additional perimeter security actions may be identified as a result of incident review if a security breach occurs.

- **Transit Centers and Park/Ride Facilities –** Rail transit parking garages are equipped with CCTV surveillance. In general, Transit Security Officers (non-sworn contracted security personnel), Transit Police Officers, and Field Operations Supervisors patrol the park/ride facilities according to deployment plans based on analysis of transit crime data and intelligence. Warnings and Citations are issued for infractions of parking rules. Suspicious activity is identified through undercover operations, CCTV surveillance, and reports from employees and passengers. "Be Alert" and "Transit Watch" notifications are posted in all transit centers, to encourage passenger security awareness. The notifications ask passengers to notify the vehicle operator or other rail transit employee of suspicious objects or activity.
- **Stations and Right of Way –** Security features include: Operations Control Center, Radio Communications, and Supervisory Control and Data Acquisition (SCADA) System, CCTV surveillance is installed at most rail transit stations, intrusion detection devices on key portals and cross-passages in tunnels monitored at the Operations Control Center, public telephones at rail transit stations provide 9-1-1 access to customers for emergencies. "Be Alert" and "Transit Watch" notifications are posted in all stations, to encourage passenger security awareness. The notifications ask passengers to notify the vehicle operator or other rail transit employee of suspicious objects or activity, SOPs and employee training reinforce constant vigilance and observations of the right-of-way and facilities by rail operators and field supervisors. Transit Police, Transit Security Officers, and Fare Inspectors are deployed along the rail transit system daily according to regular deployment schedules and special tactical missions.
- **Design and Construction of Extension Projects and Modifications --** The design development process includes design reviews by operations managers, including the agency's safety and security/police function. Crime Prevention Through Environmental Design (CPTED) principles, including FTA's Transit Security Design Considerations, are applied to light rail facilities design to enhance security, such as through open sight lines, lighting levels, etc., enforced through the safety and security certification process. Ongoing security assessments or incident reviews may identify design changes sometimes needed at existing stations to improve security are performed.
- **Operations Control Center --** Rail controllers staff the Command Center all hours, all days. SOPs and Rulebooks, combined with training of all operations personnel, real-time communications with all personnel involved in the movement of trains or working in the right-of-way, and a contemporary SCADA monitoring and control system, are the foundation of both safety and security of the light rail system operations. The SCADA system displays the locations of all trains, remotely controls trackway and tunnel equipment systems, and provides alarm and fault indications for equipment systems. Rail controllers use dedicated radio, telephone, and automatic pager systems to rapidly mobilize field supervisors, and via 9-1-1, police, fire and other emergency responders for safety or security incidents on the rail system.

- **Communications –** The rail transit agency uses an 800 MHz trunked radio system for rail operations (rail vehicles, controllers, operators, and rail field supervisors) and non-revenue vehicles. The 800 Mhz radios are programmed with numerous talkgroups dedicated to regular operations and tactical/incident command functions, as well as many local government talkgroups for interoperable radio communications during incidents on or involving the rail transit system, including local law enforcement and fire/emergency medical services throughout the rail transit agency's service area. This 800 Mhz radio system provides good radio communications capability for normal and incident operations, and good radio interoperability among the rail transit agency and emergency responder organizations. Note: The 800 MHz trunked system is used for voice communications only; at the current time, it is not configured for data communications.

3.0 SEPP Management Activities

The purpose of Chapter 3 is to identify responsibilities for managing the rail transit agency's SEPP program, including its conception, development, implementation, evaluation, review, and update. This Chapter will first identify responsibilities of senior management for specific functions necessary to create the SEPP and its supporting program. Then, responsibilities for SEPP implementation will be detailed for the security/police function, for the other rail transit agency departments/functions, and by job title. The role of external agencies in supporting SEPP development, implementation and evaluation will also be explained. Finally, this chapter will describe the committee(s) established by the rail transit agency to manage and coordinate security issues across departments/functions.

3.1 Responsibility for Mission Statement and System Security Policy

- ***Element:*** *Identification of the person(s) responsible for establishing transit system security and emergency preparedness policy and for developing and approving the SEPP.*

This section should define the authority and responsibility for the security organization, including but not limited to:

- designate and list the individual(s) responsible for determining security policy on behalf of the system and for carrying out the SEPP; and
- define the security/police function's mission and role in the organization.

Typically, this section of the SEPP will discuss the role of the General Manager in preparing, revising, reviewing and signing the policy statement and the role of the head of security/police function and his or her staff in preparing, revising and reviewing the SEPP. *It should be noted that annual reviews are now required by FTA's 49 CFR Part 659 and the state oversight agency, regarding a determination of whether the SEPP should be updated*. The head of the security/police function is typically responsible for ensuring that this annual review is performed and that the results are conveyed to the state oversight agency according to procedures and time-frames

specified in the oversight agency's Program Standard. This section may quote or reference the *SEPP Memorandum of Executive Approval/System Security Policy*.

3.2 MANAGEMENT OF THE SEPP PROGRAM

- ***Element:*** *Identification of the person(s) with overall responsibility for transit security and emergency preparedness, including day-to-day operations, SEPP-related internal communications, liaison with external organizations, and identifying and resolving SEPP-related concerns.*

This section of the SEPP needs to identify the person or people in charge of managing transit security and emergency preparedness and the SEPP program. Two basic structures for managing the program are possibly dependent on the size of the transit system. In a small rail transit system that lacks its own police or security department, the General Manager or Operations Manager may play a large role not only in setting SEPP policy, but in actually overseeing the plan and carrying it out on a regular basis.

In larger rail transit systems, although the General Manager is ultimately responsible and accountable for system security and emergency preparedness, it is expected that another individual, most likely the Manager or Chief of the security/police function, will be responsible for coordinating the daily activities outlined in the SEPP. Other individuals within the security/police function may be designed to support the Manager or Chief in overseeing implementation of the SEPP.

Although it may appear self-evident which arrangement governs the plan, this section should state clearly and unequivocally which structure is in effect and should present the general reporting responsibilities regarding security for the entire organization. Specifically, this section should address who is responsible for these ten critical SEPP management activities:

1. Defining ultimate responsibility for secure rail transit system operations.
2. Communicating that security is a top priority for all rail transit employees.
3. Advocating for, and allocating security program resources; directing day-to-day security operational activities (including tactics, intelligence and analysis); and assessing security performance.
4. Developing and explaining relations with outside organizations that contribute to the rail transit agency's security and emergency preparedness program.
5. Developing relations with local, state and federal security-related agencies, including security oversight roles of FTA's state Safety Oversight and Project Management Oversight (PMO) programs, security oversight role of DHS TSA, and emergency preparedness roles of DHS G&T, the state Office of Homeland Security, the region's emergency management group or committee, and Urban Area Security Initiative, Point-of-Contact Working Group.
6. Explaining the mechanism for bringing security concerns to the attention of the appropriate rail transit agency official or group.
7. Identifying potential security concerns in any part of the rail transit agency's operations.
8. Actively soliciting the security concerns of employees.

9. Explaining the liaison between rail transit employees and other security and emergency preparedness groups, committees and functions at the rail transit agency, for the purpose of addressing employees' security concerns.
10. Working to ensure the rail transit agency's security and emergency preparedness program is carried out on a daily basis.

A matrix could also be used to present these 10 activities and to identify which management positions have responsibility for their implementation (i.e., General Manager, Manager, the Manager or Chief of the security/police function, the Commander of the Transit Police Division, the rail transit agency's Security Committee(s), the heads of various rail transit departments/functions, and operations and maintenance supervisors).

3.3 DIVISION OF SECURITY RESPONSIBILITIES

3.3.1 Security/Police Function Responsibilities

- ***Element:*** *Listing of SEPP-related responsibilities of the personnel who work within the transit agency security/police function.*

This section should present a detailed description of the security/police function, including staff, the qualifications of the personnel, any planned short- or long-term additions to the security organization's mission, and any additional staff which may be required. Specific roles and responsibilities should also be identified.

In preparing this section of the SEPP, the rail transit agency should consider including:

- an organization chart of the transit agency's security/police function if not provided in Section 2.2 or included in an Appendix that is referenced in Section 2.2 or this section;
- a description of the number of employees in the security/police function and their job categories (i.e., Manager/Chief of Police, Access Control Coordinator, Security Data Coordinator, Homeland Security Coordinator, sworn police officers (by rank – Police Officer, Sergeant, Lieutenant, Captain, Commander, etc. or unit), non-sworn contracted or in-house security personnel (by title or unit, i.e., fare inspectors, guards, etc.), Deputy District Attorney, other specialized personnel, etc.;
- the fiscal year operating budget for the security/police function; and
- a description of the security/police roles and responsibilities for each category of job.

In addressing this last category, the rail transit agency may consider the following examples.

In describing the roles and responsibilities of the **Manager or Chief of the security/police function**, the rail transit agency may identify the following activities:

- coordinates security personnel deployments, tactics and protocols for optimal security effectiveness;

- coordinates and chairs the rail transit agency's Proactive Security Committee and Security Breach Review Committee;
- coordinates and leads planning for the rail transit agency's SEPP program development;
- coordinates with local law enforcement agencies, and ensures the development of formal memorandum of agreement/understanding;
- directs development and delivery of employee security awareness and training;
- manages security threats and vulnerabilities for current operations and for new start projects;
- oversees Crime Prevention Through Environmental Design (CPTED), security design criteria and certification process for new start projects;
- oversees the agency's facilities access control program;
- oversees security incident reporting, investigation and trend analysis;
- manages security independent audits and security corrective action plans;
- directs and coordinates the agency's emergency preparedness program, providing for plans, organization, equipment, training/procedures, and exercises/evaluation, for preparedness to perform the prevention, detection, response and recovery capabilities applicable to mass transit employees and operations during catastrophic natural disasters or terrorist attacks, appropriately coordinated/integrated with emergency response/management jurisdictions in the agency's service area;
- assures that all rail transit agency security and emergency preparedness programs meet or exceed applicable regulations and guidance of the FTA and DHS;
- serves as the agency's lead liaison/representative for security-related functions of FTA's state safety oversight program and project management oversight program, and for coordination and integration of emergency plans with emergency response/ management jurisdictions in the agency's service area, and for responsiveness to DHS incident management and national preparedness directives; and
- coordinates with the state oversight agency.

The security functions and responsibilities of the **Commander, Transit Police Division** may include:

- line authority for deployment and command of transit police officers and security officers;
- department-head responsibility for allocation of Transit Police Division resources, operational activities (including tactics, intelligence and analysis), and performance;
- law-enforcement representative on rail transit agency's Security Committee; and
- works with the other rail transit agency departments in: ongoing assessment and development of the transit SEPP program and representing the rail transit agency's security interests with other governmental jurisdictions and agencies.

In another example, **Transit Police Officers** may be responsible for:

- knowing the law, and regulations governing the enforcement of law;
- exercising discretion and good judgment;
- conducting high visibility patrols of rail transit property to enforce laws, ordinances, and codes;
- responding to emergency incidents and taking appropriate action;
- mutual liaison and assistance with law enforcement personnel throughout the agency's service area;
- developing and conducting targeted enforcement and apprehension missions on the transit system in collaboration with the Rail Operations department and other local law enforcement jurisdictions;
- assessing threats and vulnerabilities on the transit system and facilities and recommending corrective measures to reduce potential crime and vulnerability on the system;
- conducting investigations of misdemeanor and minor felony crimes;
- assisting rail transit agency staff in other departments in developing security-related operating procedures, training, and customer/public information;
- receiving security threat and crime intelligence through law enforcement sources in the region, continually and concurrently, for assessment and incorporation into security/police function resource deployments and tactics and agency Operations Orders;
- conducting security assessments and inspections of agency operations and facilities;
- coordinating the use of CCTV surveillance systems throughout the rail transit system to support investigations, apprehensions and prosecutions; and
- performing CPTED reviews of designs for new service projects or operating facilities.

3.3.2 Security Responsibilities of Other Departments/Functions

- ***Element*****:** *Listing of SEPP-related responsibilities of other departments/functions, including their relationship to the security/police function.*

This section of the SEPP should provide an overview of the other rail transit agency departments/functions that support the security/police function in implementing the SEPP. This section should contain a narrative description of the general roles and responsibilities performed by each department/function and how that department/function interfaces with the security/police function. As a guideline, no more than two or three paragraphs should be devoted to describing the security responsibilities of each other department/function within the rail transit agency.

3.3.3 Job-specific Security Responsibilities

- ***Element*: *Listing of security-related responsibilities for other (non-security/police) rail transit agency employees, including their relationship to the employee's other duties.***

This section should review and list the titles of all line and staff positions of the other departments/functions within the transit system and summarize their respective security responsibilities. In preparing these lists, rail transit agency's may to consider the following examples.

Rail operators have an important role in system security and emergency response. They are expected to:

- At beginning of service and the end of lines/routes or shifts, inspect vehicles and/or facilities for suspicious packages/items and unsafe conditions/defects.
- While in service, observe/recognize unusual/suspicious conditions or emergency incidents.
- Report any unusual conditions or emergency incidents or accidents in accordance to the Operations Control Center (OCC) in conformance with SOPs and Rulebook.
- Determine when to call (via vehicle or portable radio) the OCC for assistance.
- Respond to information or requests from passengers concerning security. On rail vehicles, passengers contact the operator via emergency intercom from the passenger compartment.
- Be alert and observant of the personal security of rail transit system employees, customers, and the general public at stations, stops and along the route of their vehicle.
- In the event of an accident or security incident, perform initial situation assessment and provide OCC and the security/police function with information regarding what has happened, the vehicle number, location, route/direction, and information regarding fatalities, injuries or other relevant conditions.
- Identify and report any immediate safety concerns at the scene (fire, fuel leak, status of suspicious package, etc.).
- If involved in an accident, provide sufficient information to OCC to classify the accident status and identify required resources.
- Establish initial transportation agency response at scene, including evacuation of vehicle or facility (if necessary) and protection of passengers, employees, contractors and/or property at the scene (following SOPs and Rulebook).
- Communicate with passengers, provide clear directions, and offer updates and passenger assistance at the scene.
- Follows instructions from OCC.
- Collect information, including the names of as many affected passengers as possible and others who may have been involved in the incident/accident, and distribute Courtesy Cards to passengers.

- Provide updates to OCC.
- Request resources (as appropriate).
- Wait for/meet supervisor and other rail transit responders at scene.
- As appropriate, briefs supervisor/other responders at scene.
- Assume control of the scene of a security incident (acting on-scene incident commander) until arrival of a rail supervisor, emergency personnel or security/police function personnel.
- Report all security incidents to the OCC, including observations of new vandalism damage or major or offensive graffiti.
- Provide security-related written reports to the OCC.
- If appropriate, coordinate with supervisor and on-scene emergency responders to support the protection of passengers, employees, contractors and other who may be affected.
- Collect information from emergency responders regarding city, badge numbers, and the numbers of responder vehicles.

Rail supervisors have specific security and emergency responsibilities as well as a general responsibility for monitoring employees' compliance with the agency's security procedures. For this reason, rail supervisors should have full knowledge of security rules and procedures, and should communicate them on an ongoing basis so as to encourage other employees to incorporate security practices into their daily work activities. Specifically, rail supervisors are to:

- Respond to security and emergency incidents.
- Report observations of new vandalism damage or major or offensive graffiti to the Operations Control Center.
- Act as the on-scene incident commander for the rail transit agency.
- Act in conjunction with the ranking or designated police authority in a unified incident command structure according to Incident Command System (ICS) procedures.
- Provide leadership and direction to employees during security incidents.
- Provide liaison with local or transit law enforcement officers and assist, when asked, in crowd control, securing witness information, and providing general on-scene assistance (but no physical involvement in violent behavior, when avoidable).
- Make on-scene decisions about restricting or continuing operations and requesting resources.
- Prepare and submit reports for security incidents in which they are involved or to which they respond.
- Identify and report security threats and vulnerabilities.
- Collaborate with the system safety and security/police functions in assessing security threats and vulnerabilities, and trends in security breaches.

- Collaborate with transit security/police responders and local law enforcement in enforcement missions.
- Follow radio communication protocols for internal and outside agency talk groups.
- De-energize rail car(s) and overhead catenary, as applicable.
- Apply hand brakes or secure rail car(s) to prevent unintended movement of same.
- Ensure that sufficient resources are en route to the scene.
- Support the protection of passengers, employees, vehicles and property at the scene.
- Requests alternate means of transportation for passengers if required.
- Meet arriving rail transit agency resources and emergency responders at the scene, and provide briefings as required.
- Support the establishment of staging areas.
- Support the security/police functions and local emergency responders at the scene in addressing the needs of injured passengers/employees and in isolating the scene.
- Provide updates to OCC.
- Request additional resources (if necessary) based on the evolving incident/accident scene.
- Block the scene (as appropriate) and secures the affected vehicle/location to prevent people from entering.
- As appropriate, ensure that the evidence and physical circumstances at the scene are preserved as much as possible.
- Ensure that activities have been performed to identify affected passengers/employees, to distribute Courtesy Cards, and to collect information from passengers and arriving emergency responders.

Rail controllers are expected to:

- Dispatch rail supervisory personnel.
- Receive and respond to calls for assistance during security and emergency incidents.
- Call 9-1-1 emergency communications centers for local law enforcement and emergency response, and transit security/police response in emergency situations, convey information in an accurate and timely manner.
- Prioritize emergency and non-emergency calls for assistance.
- Maintain communications, location and status of agency system safety and security/police function personnel.
- Prepare and submit reports for security incidents to which they respond.
- Make appropriate paging notifications to chain-of-command, public information and other agency personnel, according to incident notification procedures.
- Address requests for support through notification and dispatch of resources.

- Perform action necessary to manage rail transit service in and around the affected area, including suspension of service, re-routing of service, diversions, and bus bridges/shuttles.
- Coordinate information regarding service changes with rail transit field personnel and with the on-scene response.
- Manage the elements of the transportation system not affected by the emergency.
- Coordinate with the security/police functions and other responding agency dispatch centers regarding resource requests and requirements.
- As appropriate, convey requests to and from local/county Emergency Operations Center(s).
- Support the preparation of incident summary information for use by Media Relations.
- Monitor and respond to intrusion or security alarms and CCTV incidents. Operate CCTV recording system for monitored facilities. Following CCTV recording chain-of-custody procedures, remove and transfer recordings to authorized recipients, and order vehicle maintenance departments to remove/transfer vehicle CCTV recordings to authorized recipients.
- Develop and issue Operations Orders for special events or situations calling for non-normal transit system operations, including applicable security considerations developed in collaboration with the system safety and security/police functions.
- Monitor the transit system's building access control system alarms; coordinate with the security/police function for resolving problems.

3.3.4 Security Task Responsibilities Matrix

- ***Element:*** *A SEPP Program Roles and Responsibilities Matrix should be developed showing interfaces with other transit system departments/functions and the key reports or actions required.*

A security task responsibilities matrix should be presented showing interfaces and the key reports or actions required, including the frequency of those reports or actions. An example of a security task matrix, organized by SEPP section, is displayed below.

SEPP PROGRAM ROLES AND RESPONSIBILITIES MATRIX

TASK OR ACTIVITY **P** - Primary Responsibility **S** - Support Responsibility **A** - Approval **C** - Review and Comment	TRANSPORTATION SYSTEM							
	Management	**Operations**	**Maintenance**	**Security/ Police**	**Training**	**Engineering**	**Human Resources**	**System Safety**
System Security Program Introduction	A	A	C	P	C	C	C	C
Purpose of System Security Program Plan and Program	A	A	C	P	C	C	C	C
Goals, Objectives, & Tasks for the Program	A	A	C	P	C	C	C	C
Scope of Program	A	A	C	P	C	C	C	C
Security & Law Enforcement	A	A	C	P	C	C	C	C
Management Authority & Legal Aspects	A	A	C	P	C	C	C	C
Government Involvement	A	A	C	P	C	C	C	C
Security Definitions	A	A	C	P	C	C	C	C
System Description	C	C	C	P	C	C	C	C
Background & History of System	C	C	C	P	C	C	C	C
Organizational Structure	C	C	C	P	C	C	C	C
Human Resources	C	C	C	P	C	C	C	C
Passengers	C	C	C	P	C	C	C	C
Services and Operations	C	C	C	P	C	C	C	C
Operating Environment	C	C	C	P	C	C	C	C
Integration with Other Plans	C	C	C	P	C	C	C	C
Current Security Conditions	A	A	C	P	C	C	C	C
Capabilities & Practices	A	A	C	P	C	C	C	C
Management of the System Security Plan	A	A	C	P				C
Responsibility for Mission Statement & System Security	A	A	C	P	C	C	C	C
Management of the Program	A	A	S	P	S	S	S	S
General Manager	A	C	S	S	S	S	S	S
Chief Operating Officer	A	A	S	S	S	S	S	S
Division of Security Responsibilities	A	A	C	P	C	C	C	C
Job-specific Security Responsibilities	C	A	S	P	S	S	S	S
External Agencies	S	S	S	P	S	S	S	S
Security Committees	C	A	S	P	S	S	S	S
SEPP Program: Roles & Responsibilities	C	S	S	P	S	S	S	S
Planning	S	S	S	P	S	S	S	S
Proactive Measures	S	S	S	P	S	S	S	S
Training	S	S	S	P	S	S	S	S
Day-to-Day Activities	S	S	S	P	S	S	S	S
Security Program Threat & Vulnerability Management	C	P	P	P	C	P	S	C
Threat & Vulnerability Identification	C	P	C	P	S	S	S	C
Security Testing and Inspections	C	P	C	S	S	S	S	C
Data Collection	C	P	S	S	S	S	S	S
Reports	C	P	S	S	S	S	S	S
Security Information Flow	C	P	S	S	S	S	S	S
Threat & Vulnerability Assessment	C	C	S	P	S	S	S	S
Responsibility	C	C	S	P	S	S	S	S
Data Analysis	C	F	S	P	S	S	S	S
Frequency & Severity	C	C	S	P	S	S	S	S
Threat & Vulnerability Resolution	C	P	C	P	S	S	S	S
Emergency Response	A	A	S	P	S	S	S	S
Breach Investigation	A	A	S	P	S	S	S	S
Research and Improvements	A	A	S	P	S	S	S	S
Eliminate, Mitigate, or Accept	A	A	S	P	S	S	S	S
Implementation & Evaluation of System Security Program Plan	C	P	C	P	S	S	S	C
Implementation Goals & Objectives	C	P	C	P	S	S	S	C
Implementation Schedule	C	P	C	P		S	S	C
Evaluation	C	P	C	S	S	S	S	S
Internal Audit – Management	C	C	C	P	S		S	
External Audits	S	P	S	S	S	S	S	S
Modification of the System Security Program Plan	S	P	S	S	S	S	S	S
Initiation	C	C	S	P	S	S	S	S
Review Process	C	P	S	P	S	S	S	S
Implement Modifications	P	P	S	P	S	S	S	S

For rail transit agencies choosing to take another approach, the task matrix can also be organized by specific tasks identified to implement the goals and objectives presented in Section 1.2. Or, as an alternate approach, rail transit agencies can organize their task matrices using a combination of specific activities to be performed to achieve goals and objectives and the SEPP plan organization.

3.3.5 Responsibilities of External Agencies

- ***Element*****:** *The responsibilities of external agencies for supporting SEPP development and implementation should be identified.*

This section should briefly identify the external agencies that the rail transit agency works with in implementing its SEPP. As appropriate, reference may be made to Section 1.6 (Government Involvement) of this plan. For each external agency listed, this section of the SEPP should identify their specific responsibilities in supporting the SEPP (i.e., providing funding, training or technical assistance, reviewing and approving plans, etc.).

In addition, this section of the SEPP should also describe the rail transit agency's relationship with the state safety oversight agency. This section should briefly summarize the requirements specified by the state oversight agency for SEPP development and implementation and other security activities, and the activities that must be performed by the state oversight agency.

The role of G&T and TSA in reviewing the SEPP should also be specified.

3.3.6 Security Committees

- ***Element:*** *The committees developed by the rail transit agency to address security issues should be identified.*

This section of the SEPP should identify the committee or committees established by the rail transit agency to address security issues. In the rail transit environment, the security committee(s) generally reports to top management through the chief operating officer or director of operations. The major task of this committee(s) is to identify and resolve potential security risks that the transportation system may encounter during operations. In preparing this section, the rail transit agency may consider the following example:

Coordinating and leading planning for the rail transit agency's SEPP program development is an essential job function of the Manager or Chief of the security/police function. In performing this activity, the Manager or Chief chairs the rail transit agency's Security Committee, consisting of the following:

- Executive Director, Operations
- Commander, Transit Police Division
- Manager, Field Operations
- Director, Transportation Operations
- Director, Operations Training
- Director, Facilities Management
- Director, Operations Planning and Development

- Asst. General Counsel, Compliance and Policy

The Security Committee also includes two rail operator representatives and one front-line maintenance employee representative.

Members of the Security Committee, in their respective security-related functional roles, contribute directly to planning the security and emergency preparedness program. The Security Committee meets at least once monthly. It extends the scope and effectiveness of the management of the security program, by assuring involvement and collaboration of all rail transit agency departments/functions in security program development and implementation, and by advising on development and evaluation of the program.

Security Committee meetings include reviews of:

- security incidents;
- proposed improvements in security procedures, equipment and training;
- changes to transit agency facilities or operations affecting security;
- security information related to upcoming events in the region affecting the transit system;
- trends in transit system crime data; and
- security assessments of transit agency operations and facilities.

4. SEPP Program Description

Chapter 3 identified the rail transit agency's approach to managing the SEPP, and specified the SEPP-related responsibilities of management and line positions within the security/police function and the other rail transit departments/functions. Chapter 4 demonstrates how the SEPP management functions and responsibilities identified in Chapter 3 are integrated into a cohesive and effective program. The elements of this program are presented using the POETE categorization specified by DHS/TSA and G&T in implementing the National Preparedness Goal: Planning, Organization, Equipment, Training/Procedures, and Emergency Exercises and Evaluation. Examples for how rail transit agencies could address each of these five categories of activities are provided in Sections 4.1 through 4.5 below.

<u>NOTE</u>: In describing implementation of the SEPP program, rail transit agencies who are not participating in the G&T Transit Security Grant Program may use the traditional categories, previously recommended in FTA guidance: Planning, Proactive Measures, Training, and Day-to-Day Activities. Or these rail transit agencies may choose to use the POETE categories, since either organizational scheme provides the same general information.

4.1 PLANNING

- ***Element:*** *Identification of SEPP activities and programs in place at the rail transit agency to support planning for system security and emergency preparedness.*

Planning for the SEPP program includes developing internal agency plans to address SEPP issues during rail transit agency operations; budgeting for system security and emergency preparedness functions; addressing security requirements in system design and safety/security certification for extensions and major projects, renovations and rehabilitations; and coordinating with local emergency management agencies and public safety agencies to ensure integration of the rail transit agency into response community plans for major criminal events, terrorist activities (including the use of Improvised Explosive Devices [IEDs] and the release of Chemical, Biological, Radiological, Nuclear and Explosive [CBRNE] agents), and natural disasters.

Internal Planning: Planning is an integral part of maintaining and operating a secure rail transit system. Stemming from state safety oversight requirements and DHS/G&T regulations and requirements, the rail transit agency has developed a set of plans to document its combined activities to address issues affecting the safety and security of passengers and employees, the agency's ability to protect its infrastructure from crime and terrorism, and the agency's capabilities to provide effective emergency response to a wide range of emergencies. To this end, the rail transit agency has developed this SEPP, as well as a *System Safety Program Plan*, a *System Safety and Security Certification Program Plan*, an *Emergency Operations Plan*, and a set of *Incident Specific Response Plans* for severe weather and natural disaster, a range of accident types and fires, and major crimes and terrorism.

Wherever possible and appropriate, these plans address state oversight agency requirements as well as DHS Homeland Security Presidential Directives (HSPDs) requiring implementation of the National Response Plan, the National Incident Management System, the National Infrastructure Protection Plan, and the National Preparedness Goal. In addition, the results of internal and external assessments performed at and by the agency addressing SEPP-related issues are also integrated into these plans, including needs assessments and threat and vulnerability assessments.

Budgeting: The rail transit agency's annual capital budget recommendations are developed by a senior staff group called the Capital Committee. The Executive Director, Operations is represented on the Capital Committee by the Director, Operations Planning and Development, who assures that the security capital improvement needs are incorporated into the rail transit agency's annual capital budget development process and 5-year Capital Improvement Program (C.I.P.) forecast. The rail transit agency's security/police function provides an annual budget request. Rail transit agency committees also identify needed security and emergency preparedness improvements and make recommendations to the Director, Operations Planning and Development. Finally, the results of needs assessments and regional plans for communications interoperability and terrorism early warning systems are also shared with the Capital Committee.

Security Requirements in Design: The rail transit agency addresses security in planning for system modifications, extensions and rehabilitations. Using selected design features and technologies, crime and terrorism prevention capabilities are accomplished through an integrated approach based on CPTED principles. The rail transit agency requires all drawings and

specifications to be reviewed by an American Society for Industrial Security (ASIS) Board Certified Protection Professional (CPP) who reviews them for CPTED concepts and upon acceptance, stamps the drawings and approves the specifications. Security reviews are conducted throughout the design process, and during construction, security features are assessed for their compliance with specifications, prior to being accepted and placed into service. The security/police function has both formal and informal input into design decisions that affect passenger, employee, and equipment security. In addition, the rail transit agency has developed Security Design Criteria, which ensure that CPTED principles are applied to all aspects of facilities and vehicle design. FTA's *Transit Security Design Considerations* is incorporated by reference into the design criteria, as a comprehensive CPTED guide.

The rail transit agency's security planning in development of new transit projects is formalized through the Safety Certification Program. As described in the rail transit agency's *System Safety Program Plan* and *System Safety and Security Certification Program Plan*, the rail transit agency conducts a safety certification process to ensure that safety concerns and hazards are adequately addressed prior to the initiation of passenger operations for new start rail transit projects and for major modifications to rail transit systems. The intent and practice of the safety certification program is that security considerations are integrated into the safety certification process, in the same manner as safety considerations.

To conduct this process, the rail transit agency specifies use of its security design criteria, a set of safety and security design reviews performed by several groups devoted to safety and security issues, including the Safety and Security Task Force, Fire/Life Safety and Security Committee, contracted safety and security engineering support, the rail transit agency's system safety and security/police functions, and the agency's standing committee for configuration management, and an extensive verification process to ensure that security elements specified in the design are actually built into the delivered project. Testing, start-up, training and emergency readiness issues are also addressed in this process.

Coordination for Regional Emergency Preparedness Capabilities: Following the events of September 11, 2001, and all subsequent DHS directives and guidance calling for a permanently heightened level of security awareness and emergency preparedness, officials from the rail transit agency have been working closely with officials of the region's emergency management organizations to: (1) include the rail transit agency as a full-fledged member of regional organizations and working groups established by emergency management and public safety organizations for purposes of planning and preparing for regional emergency responses, and (2) assure appropriate inclusion of the rail transit agency in the emergency response and security alert procedures of the region's Emergency Operations Centers.

The rail transit agency has coordinated with both local and county governments and the emergency management agencies in its service area to support on-going development and revision of their respective Emergency Operations Plans and supporting incident management and response protocols and resource inventories. The rail transit agency has also partnered with the major municipality in its service area to develop a *Downtown Evacuation Plan*, to ensure effective response to no-notice evacuations and emergencies, including events related to IED and CBRNE, earthquakes, fires and flooding.

The rail transit agency has established MOUs with local law enforcement, emergency medical services, fire departments, hospitals and other transit providers in the region. These MOUs provide direction and clarification regarding response to an incident occurring on the rail transit agency, and how the rail transit agency may support response to area-wide emergencies.

In addition, the rail transit agency, working with the Regional Transit Security Working Group and the region's Urban Area Security Initiative agencies, has developed and implemented the Regional Transit Security Strategy. The RTSS provides the integration point between the individual, risk-based SEPPs of the rail transit agencies in the region, and the overall security goals and objectives established for the region. The RTSS demonstrates a clear linkage to the applicable state and urban area homeland security strategies developed or currently being developed. For G&T's Transit Security Grant Program, it is expected that the SEPPs and the RTSS will serve as the basis on which funding is allocated to address regional transit security priorities, and the vehicle through which the rail transit agency may justify and access other funding and resources available on a region-wide basis through the UASI program.

4.2 ORGANIZATION

- ***Element:*** *Identification of the organization of SEPP-related activities and programs and the ability to coordinate with external response agencies.*

Capabilities for the rail transit agency's response to major crimes, terrorism and natural disaster emergencies are organized following the *Incident Management Organization* specified in the rail transit agency *Emergency Operations Plan*, as well as the procedures identified in rail rulebooks and SOPs/Emergency Procedures, the agency's Crisis Communications Plan, the security/police function's General Orders, the agency's Incident Specific Response Plans, and internal transit facility emergency emergency/evacuation plans. The rail transit agency's *Incident Management Organization* provides an organized command and control structure to ensure (1) coordinated response across the agency's departments/functions and (2) adequate resources are mobilized during emergency incidents. The rail transit agency's *Incident Management Organization* is akin to the Incident Command System (ICS) used by local responders. This organization enables the rail transit agency to integrate effectively with the ICS established by public safety and emergency management agencies, complying with the terms of both NIMS and the Major Emergency Incident Management System protocols established for the regional area.

These capabilities are coordinated and integrated with external jurisdictions and regional emergency preparedness plans, such as the municipal and county Emergency Operations Plans and the Downtown Evacuation Plan. Specific rail transit agency capabilities are also documented in the Regional Transit Security Strategy.

Specifically for terrorism, the rail transit agency recognizes that unique capabilities are provided by public safety responders in the region for addressing a range of terrorism-related events, including CBRNE and IED events occurring on or adjacent to rail transit property. Further, as specified in the Regional Transit Security Strategy, the rail transit agency has identified these capabilities and also has established its own resources to prevent, detect, respond to and recover from these events.

The organization of terrorism or emergency incident response teams in the rail transit agency's service area includes the following capabilities: canine teams, explosive ordinance disposal, hazardous materials, underwater dive teams, special weapons and tactics, emergency medical services, medical surge teams, and urban search and rescue. These teams are available throughout the rail transit system's service area.

Capabilities to collect, analyze, and disseminate information on potential threats to the region's transit systems include:

- Transit security/police function participates in the region's Federal Bureau of Investigation (FBI)/Joint Terrorism Task Force (JTTF). Any information relating to potential transit threats is promptly forwarded through this function.
- Transit security/police function is establishing a Homeland Security Unit, including an officer dedicated to intelligence fusion and analysis and coordination with other law enforcement agencies in the region, state and national level.
- Transit security/police function receives advisories from DHS (including G&T and TSA) as well as information transmitted by Federal Transit Administration and the U.S. Department of Transportation.
- Local police intelligence is continually shared with the tail transit security/police function.

An additional capability desired is inclusion of public transportation agencies in development of a Terrorism Early Warning (TEW) system for the region. The state Office of Homeland Security is establishing a Strategic Analysis Information Center (SAIC) to effectively collect and share information from many different sources. The SAIC is designed to integrate existing local, state and federal information systems to create a central "fusion" center. The center will partner with many different sources of information, fusing relevant information and distributing valuable information to private and public sectors, first responders and investigators.

Policies or procedures to coordinate within this organizational structure to share information include:

- Using an 800 Mhz regional system owned by the municipality/state that enables cross-communication through defined talk-group templates.
- The region is developing an interoperability plan per HSPD-8 addressing Computer Aided Dispatch (CAD)/data system and radio cross-communication among its county/city 9-1-1 centers; the rail transit agency is a participant in developing the region's HSPD-8 and G&T-required tactical interoperability communications plan (TICP).

4.3 EQUIPMENT

- ***Element:*** *Description of the equipment used to support implementation of the SEPP program.*

Through the administration of DHS and FEMA grants in the rail transit agency's service area, first responders have obtained equipment, training and certification to support response to security and CBRNE events as well as natural disasters. Regional procedures, drills and exercises are being developed to ensure these capabilities. Through the state Emergency Management Agency, this activity has been coordinated with the Terrorism Annex of the state Emergency Operations Plan, as well as the state Homeland Security Assessment and Strategy. Based on the results of this assessment and strategy, specific equipment needs have been identified, prioritized and are being addressed in each of the state's counties and major municipalities. Regional UASI working groups are also coordinating with the state Senior Interagency Coordinating Group (SICG) and the state Security Task Force to address the need to achieve greater terrorism and natural disaster preparedness and to work toward statewide response capabilities, including the acquisition of additional equipment.

The rail transit agency also has equipment to support its capabilities to detect, prevent, respond to and recover from security and terrorism events and to manage natural disasters:

- CCTV equipment is installed on rail transit vehicles and in rail transit agency facilities, coordinated with the agency's access control system.
- The rail transit agency is revising its CCTV policy and may decide to equip additional stations and vehicles.
- The rail transit agency's security/police function monitors an extensive network of security, fire, duress, intrusion, utility and internal 911 alarm systems.
- Intrusion detection is installed for elevated structure access points and tunnel portals and cross-passages.
- The rail transit agency's security/police function administers an automated employee access control system and performs analysis of security data and security breeches.
- CCTV incorporated into design criteria for all new-project stations and park-rides, as of 2005.
- The rail transit agency's security/police function performs security screening of visitors and temporary visitor passes and escorts are required.
- Mail is screened at a central facility and procedures have been established for receiving deliveries from overnight services and vendors.
- The rail transit agency revised its policy for standard trashcans, following 5/20/04 TSA RAILPAX-04-01 directive.
- New non-concealing trashcan design will be adopted for future projects.

The rail transit agency also has a variety of equipment in place to ensure the integrity of the following:

- Protection against unauthorized entry:
  - Fencing for rail yard and administrative facilities.
  - Fencing at traction power substations and maintenance of way out-buildings.
  - Fencing along right-of-way.
  - Intrusion detection separating right-of-way from shared corridor operations.
  - Walls, ceilings, and windows have been assessed, and graffiti-resistant materials, locks, bullet resistant materials and anti-fragmentation materials have been installed/used at critical locations.

- Other features include:
  - Consideration given to employee, passenger and visitor traffic patterns in the design, lay-out and use of facilities and stations.
  - Standards have been established to ensure internal and external lighting levels compliance with recommendations from the American Society for Industrial Security.
  - Directional signage is provided in a consistent manner in all stations, both to provide orientation and to support emergency evacuation.
  - National Fire Protection Association Standard (NFPA) 130 is used to ensure fire/life safety in station design, including fire detection systems, firewalls and flame-resistant materials, back-up power and emergency lighting, defaults in turnstile and other systems supporting emergency exists, and pre-recorded public announcements.
  - Gates and locks are used on all facility doors to prevent unauthorized access. Keys are controlled through an established program managed by the security/police function.
  - Gates and locks are also used to close down system facilities after operating hours.
  - Rail vehicles have radios, silent alarms, CCTV, and passenger communications.
  - Uninterruptible Power Supply (UPS) or redundant power sources are provided for safety and security of critical equipment, such as but not limited to: exit and platform lighting; parking lot lighting; ancillary space and shop lighting; intrusion detection (alarmed rooms and spaces, fare collection equipment, etc.); fire detection, alarm and suppression systems; public address (shop and public areas); call-for-aid telephones; CCTV; emergency trip stations; vital train control functions; etc.

The rail transit agency has also identified the following equipment needs for optimum IED/CBRNE prevention, detection and response within the regional transit sector:

- expansion of CCTV surveillance, for prevention and detection;
- comprehensive improvements to field and the security/police function communications systems, for effective response capabilities, by being able to manage transit operations during a major incident;
- backup operations command center capability; and
- investigation of the applicability of K-9 units or robotic devices to enhance explosive detection capabilities.

4.4 TRAINING AND PROCEDURES

- ***Element*:** *Description of SEPP-related training and procedures available to ensure employee proficiency.*

Training: At the rail transit agency, training for SEPP-related topics is performed to ensure that:

- applicable management, operations, and maintenance rules, procedures, and plans are effectively documented and conveyed to those responsible for their implementation;
- manuals showing how to administer, operate, and maintain the system's safety and security equipment and facilities are understood by those responsible for their use;
- safety-related rules and procedures for management, operations, and maintenance personnel are documented and effectively implemented by all employees as required;
- emergency procedures have been developed, documented and are successfully implemented by all personnel as required, including public safety personnel (if appropriate);
- transportation personnel and local emergency responders understand the hazards of the transportation environment; and
- an adequate level of preparation is maintained for a possible emergency.

Training typically addresses rules, policies, and procedures, as well as many of the hazards in the transportation environment (e.g., live power, track and roadway safety, hazardous materials and alternate fuels, medical emergencies or blood-borne pathogen awareness, personal safety, and injury prevention). The rail transit agency also has established an emergency response agency familiarization program that provides orientation for local law enforcement, fire personnel, and medical services regarding the transportation environment and its vehicles.

The rail transit agency has performed basic security awareness or first responder awareness training, which emphasizes topics, such as:

- understanding the specific threats from explosives, incendiary devices, and toxic materials (chemical, biological, or radiological agents) and the risks associated with them in an incident;
- understanding the potential outcomes associated with an emergency created when explosives, incendiary devices, or toxic materials are present;
- the ability to recognize the presence of these devices and materials;
- the ability to identify the classes of chemical agents, if possible, using signs and symptoms;
- the ability to reference laminated cards and other automated and manual checklists to support initial response activities and incident reporting; and
- proper use of personal protective equipment, such as escape hoods and gas masks.

The rail transit agency offers a variety of training programs to support SEPP implementation, as SEPP elements are integrated into including initial and refresher training programs provided to all employees. In addition the rail transit agency provides general security awareness training to all operations and maintenance departments and holds special seminars devoted to SEPP topics with supervisors, managers and the rail transit agency's executive leadership. A brief summary of key training activities performed by the rail transit agency to address the SEPP appears below:

SEPP Training Campaigns

- All rail transit agency front-line employees, maintenance personnel and most agency staff received a four-hour security awareness training course during 2003 and 2004, prepared and delivered by the rail transit agency's training supervisors, based on the National Transit Institute's (NTI) "System Security Awareness for Transit Employees" course, sponsored by FTA.
- Rail transit agency supervisors and dedicated security personnel have received and will continue to receive specific classes devoted to SEPP-related topics, including managing security threats and workplace violence, Weapons of Mass Destruction, and NIMS/ICS, etc. For example, an NTI train-the-trainer course in Terrorist Activity Recognition and Reaction was delivered to the rail transit agency's trainers and supervisors last year, and another NTI course in Transit Response to Weapons of Mass Destruction will be delivered to the rail transit agency's trainers, supervisors and operations managers this year.
- To fulfill the next set of transit security training needs, the rail transit agency will deliver a "Phase 2" security training program, using G&T TSGP assistance. The Phase 2 security training program objectives include:
  - Deliver Behavioral Awareness Security Screening (BASS) training.
  - Deliver NIMS training, compliant with the "NIMS National Standard Training Development Guidance" issued by the NIMS Integration Center April 12, 2005, and fulfilling ICS training pursuant to the "Institutionalizing the Use of ICS" guidance issued by the NIMS Integration Center February 17, 2005.
  - Deliver training on the rail transit agency's revised Emergency Operations Plan and Incident Management Organization, including integration with regional CBRNE and other emergency management plans (e.g., earthquake).
- In early 2006, the rail transit agency will provide several versions of the "first responder awareness level" of training as defined by U.S. OSHA at 29 CFR 1910.120(q)(6)(i): "(i) First responder awareness level: First responders at the awareness level are individuals who are likely to witness or discover a hazardous substance release and who have been trained to initiate an emergency response sequence by notifying the proper authorities of the release. They would take no further action beyond notifying the authorities of the release. First responders at the awareness level shall have sufficient training or have had sufficient experience to objectively demonstrate competency in the following areas: (A) An understanding of what hazardous substances are, and the risks associated with them in an incident. (B) An understanding of the potential outcomes associated with an emergency created when hazardous substances are present. (C) The ability to recognize the presence of hazardous substances in an emergency. (D) The ability to identify the hazardous substances, if possible. (E) An

understanding of the role of the first responder awareness individual in the employer's emergency response plan including site security and control and the U.S. Department of Transportation's Emergency Response Guidebook. (F) The ability to realize the need for additional resources, and to make appropriate notifications to the communication center."

Security/Police Function:

- Security/police personnel have received security awareness training.
- Security/police personnel continue to receive training on CBRNE recognition, protective equipment, and response.
- Security/police personnel continue to receive training in CPTED and community policing techniques.
- Security/police personnel and other rail transit personnel have received training from the County Emergency Management Agency on the Major Emergency Incident Management System (MEIMS) Basic Principles and Protocols.
- Security/police personnel have also received training from local law enforcement agencies in the rail transit agency's service area regarding response to CBRNE events.

Employee Awareness:

- All employees receive security awareness training course, based on National Transit Institute (NTI) course sponsored through Federal Transit Administration.
- Security awareness training is incorporated into initial and recurrent training for all operators.
- Transportation supervisors and all dedicated personnel have received and will continue to receive specific classes on threats and SEPP-related issues (i.e., workplace violence, CBRNE, IED, etc.)
- Phase 2 of the rail transit agency's awareness training will focus on recognizing suspicious behavior, and will be provided to all front-line employees and supervisors.

Customer awareness:

- All rail transit agency vehicles are posted with Transit Watch instructions for passengers to report to Operator or other rail transit agency employee suspicious objects or persons.
- Public announcements are looped in stations directing anyone who identifies a suspicious object to report it to the nearest rail transit agency employee.

NIMS/ICS:

- The rail transit agency has updated its Incident Management Organization and supporting procedures, as specified in its Emergency Operations Plan, per NIMS guidance.
- The rail transit agency is developing a training program for its revised Emergency Operations Plan, including its NIMS-compliant Incident Management Organization.

- NIMS institutionalizing activities are in-progress at the rail transit agency for completion by 2006.
- Mutual aid and coordination relative to the rail transit agency is in process:
  - Agreements are being revised/finalized with the County Emergency Management Agency and the major municipality in the rail transit agency's service area.
  - There is an open invitation to law enforcement canine units to exercise/train on the rail transit agency's vehicles and stations.
  - The Urban Area designated for the UASI program is developing a CBRNE response plan which the rail transit agency is an integral part of. This regional plan will serve as the external-responder elements of the rail transit agency's internal CBRNE plan as well as identify public transportation tasks and capabilities needed for CBRNE preparedness.

Familiarization Training:

- The rail transit agency has provided familiarization training on its facilities, vehicles, operations and emergency response procedures to emergency management and public safety agencies in its service area.

An overview of training offered by the rail transit agency is provided below.

	Staff Level				
Courses	**Security and/or Police Function**	**Rail Controllers and OCC Supervisors**	**Operators and Station Agents**	**Operations and Maintenance Supervisors**	**Staff**
Orientation	X	X	X	X	X
SOPs, Emergency Procedures, and Emergency Operations Plan	X	X	X	X	X
Safety Rules	X	X	X	X	X
Security Awareness	X	X	X	X	X
Security Systems	X	X		X	X
- Facilities	X	X	X	X	X
- Vehicles	X	X	X	X	X
Emergency Training for 1st Responder	X[1]	X		X[2]	
Introduction to ICS/NIMS	X	X	X	X	X
Incident Command Training	X[1]	X		X[2]	
Interagency Training	X[1]	X			
Weapons of Mass Destruction/CBRNE	X[1]				
CPR	X[1]	X[3]	X[3]	X[3]	X[3]
Blood-borne Pathogens	X[1]				
First Aid	X[1]	X[3]	X[3]	X[3]	X[3]
Hazardous Material Awareness	X	X		X	

1 Pre-qualified
2 Supervisors designated as On-site incident coordinators
3 Selected Staff

Procedures: Rail operators, rail controllers at the rail transit agency's Operations Control Center, rail supervisors, transportation and maintenance personnel, and security/police function personnel use Standard Operating Procedures (SOPs) and associated Rulebooks for normal, special, and emergency operations. Most procedures supporting system security are embedded in the operations SOPs pertaining to emergency operations, communications, and response, just as system safety is embedded into operating procedures. Some security procedures are stand-alone SOPs. Training on SOPs and Rulebooks applicable to respective employee jobs is the core element of operations training for the respective jobs, serving as the primary mechanism for safety and security training for employees. To illustrate the scope of security-related and emergency management-related SOPs, a list of selected SOPs which apply to the rail operation appears below.

Example SOPs for Security and Emergency Response	
▪ Emergency Procedures Tunnel Operations/Emergencies Controller Procedures ▪ Response Protocols for Homeland Security Threat Advisory Levels ▪ Response to Threatened or Actual Acts of Terrorism, Violence or Major Incidents ▪ Unknown Substances on Vehicles and Platforms ▪ Response to Chemical Agents on Vehicles and Platforms ▪ Fire/Smoke on Train ▪ Emergency Notification Guidelines ▪ Collision or Derailment ▪ Death on Rail Transit Property ▪ Bomb Threat ▪ Earthquake ▪ Common Corridor Emergency ▪ Remote Overhead Power Removal ▪ Medical Emergency - Passenger ▪ Emergency Access to Right of Way ▪ Contact of Train and Person ▪ Incident Command System ▪ Immediate and Emergency Medical Care ▪ Fire Alarms ▪ Excessive Arcing/Broken Pantograph ▪ Emergency Vehicles ▪ Accident/Incident Reports ▪ Train Log Procedure ▪ Track Damage Assessment ▪ Loss of Radio Communications ▪ Re-Railing (except Tunnel) ▪ Confirmed Tunnel Incidents ▪ Smoke/Fire in Tunnel ▪ Tunnel Intrusion Detection/Security ▪ Tunnel Rescue Trains ▪ Tunnel Ventilation ▪ Tunnel Evacuation	▪ Tunnel Single Track Operations ▪ Tunnel Emergency Standpipe ▪ Tunnel Electrification ▪ Tunnel Person/Train Contact ▪ Tunnel Re-Railing ▪ Security Procedures ▪ Security Roles and Responsibilities ▪ Radio Usage - Security Talk Group ▪ Prohibited Conduct/Criminal Incident ▪ CCTV Procedures – Vehicles and Platforms ▪ Building Access Control ▪ TVM/Fare Maintainer Security ▪ Controlled-Access Facility Keys ▪ Controllers Emergency Procedures ▪ Coordination with Emergency Response Units ▪ Emergency Passenger Evacuations ▪ Documentation of Events ▪ Information Distribution ▪ SCADA Failure ▪ Platform PA/Readerboards ▪ Central Control System Alarms ▪ Remote Signal and Switch Operation ▪ Interface with Supervisors and Operators ▪ Central Control System Failure ▪ Rail Strategies and Restoration of Service ▪ Station Elevator Operations/Rescue ▪ Field Supervisor Procedures ▪ Rail Supervisor Responsibilities ▪ Accident/Incident Investigation ▪ Maintaining Order in Park/Ride Facilities ▪ Contingency Plan for Radio Communications ▪ Emergency Mobilization ▪ Bus Silent Alarm Response ▪ Riot/Civil Disturbance ▪ Bomb Threat ▪ Biochemical Threat/Incident ▪ Hostage or Barricade

In other procedures-related activities, the rail transit agency is:

- Establishing procedures for sweeping vehicles and stations to identify and manage suspicious items, based on HOT characteristics (hidden, obviously suspicious, not typical).
- Developing a quick reference guide for security/police personnel and other rail transit employees to use in addressing a variety of emergency situations, including the identification and evaluation of suspicious packages and conditions.
- Developing a new employee reporting procedure that assigns all operators and all other employees in field with "eyes and ears" awareness and reporting responsibilities.

The rail transit agency has also adopted specific procedures for Homeland Security Advisory System (HSAS) threat level changes; when advisory is raised, heightened security sweeps and surveillance patrols for vehicles and stations are put into effect.

Rail transit agency activity to ensure compliance with both training programs and procedures implementation is discussed in Chapter 6 of this SEPP and is also described in the System Safety Program Plan.

4.5 EMERGENCY EXERCISES AND EVALUATION

- ***Element*:** *Description of SEPP-related activities to ensure the conduct of emergency exercises and evaluation.*

Rail transit agencies are vulnerable to a range of events which may result in emergencies. The table on the following page illustrates some of the most likely of these events, organized into categories of naturally occurring and human-caused events (intentional and unintentional).

Naturally Occurring	Human-Caused	
	Intentional	**Unintentional**
▪ Droughts ▪ Dust/Wind Storms ▪ Earthquakes ▪ Electrical Storms ▪ Floods ▪ High Winds ▪ Hurricanes ▪ Ice Storms ▪ Landslides ▪ Naturally Occurring Epidemics ▪ Snowstorms and Blizzards ▪ Tornadoes ▪ Tropical Storms ▪ Tsunamis ▪ Typhoons ▪ Wildfires	▪ Bomb Threats and Other Threats of Violence ▪ Disruption of Supply Sources ▪ Fire/Arson ▪ Fraud/Embezzlement ▪ Labor Disputes/Strikes ▪ Misuse of Resources ▪ Riot/Civil Disorder ▪ Sabotage: External and Internal Actors ▪ Security Breaches ▪ Terrorist Assaults Using Chemical, Biological, Radiological or Nuclear Agents ▪ Terrorist Assaults Using Explosives, Firearms or Conventional Weapons ▪ Theft ▪ Vandalism ▪ War ▪ Workplace Violence	▪ Accidental Contamination or Hazardous Materials Spills ▪ Accidental Damage to or Destruction of Physical Plant and Assets ▪ Accidents which Affect the Transportation System ▪ Gas Outages ▪ Human Errors ▪ HVAC System Failures or Malfunctions ▪ Inappropriate Training on Emergency Procedures ▪ Power Outages ▪ Software/Hardware Failures or Malfunctions ▪ Unavailability of Key Personnel ▪ Uninterruptible Power Supply (UPS) Failure or Malfunction ▪ Voice & Data Telecommunications Failures or Malfunctions ▪ Water Outages

An exercise is a focused practice activity that places the participants in a simulated situation, which requires them to function in the capacity that would be expected of them in a real event. A good exercise, that is well evaluated, reveals inconsistencies in plans, highlights deficiencies in resources, and underscores the need for additional training.

Going directly into a real emergency operation without exercising involves substantial risks. For example, many participants may not know or thoroughly understand their emergency responsibilities and how they relate to activities performed for other elements of the response; equipment may not function as expected; or procedures may not be as effective as anticipated. Such risks, when thoughtfully considered, are unacceptable to most transportation agencies. Accordingly, a broad spectrum of exercise activity is necessary if functional emergency response and recovery capability is to be realistically assessed and improved.

Well-designed and executed exercises are the most effective means of:

- testing and validating policies, plans, procedures, training, equipment, and interagency agreements;
- clarifying and training personnel in roles and responsibilities;
- demonstrating mastery of standard and emergency operating procedures, communications, equipment, and public information dissemination;
- improving internal agency and interagency coordination and communications;
- identifying gaps in resources;

- improving individual performance; and
- identifying specific activities which should be taken to improve the response capability.

Exercises are also an excellent way to demonstrate community resolve and cooperation to prepare for disastrous events. Review of successful responses to emergencies over the years has shown that pre-emergency exercising pays huge dividends when an actual emergency occurs. This is especially true in instances where communities were involved full-scale exercises that tested the range of response activities, communications protocols, and resources to be applied.

In the rail transit environment, exercises provide an effective way to implement and fine-tune an agency's emergency plan, provide training, and improve system safety and security. Additionally, as providers of a public service, rail transit agencies have a responsibility to:

- ensure customer and employee safety and security at all times;
- train employees so they know what to do when an emergency occurs;
- recognize that they are part of the regional emergency response effort; and
- correct gaps and vulnerabilities in the system.

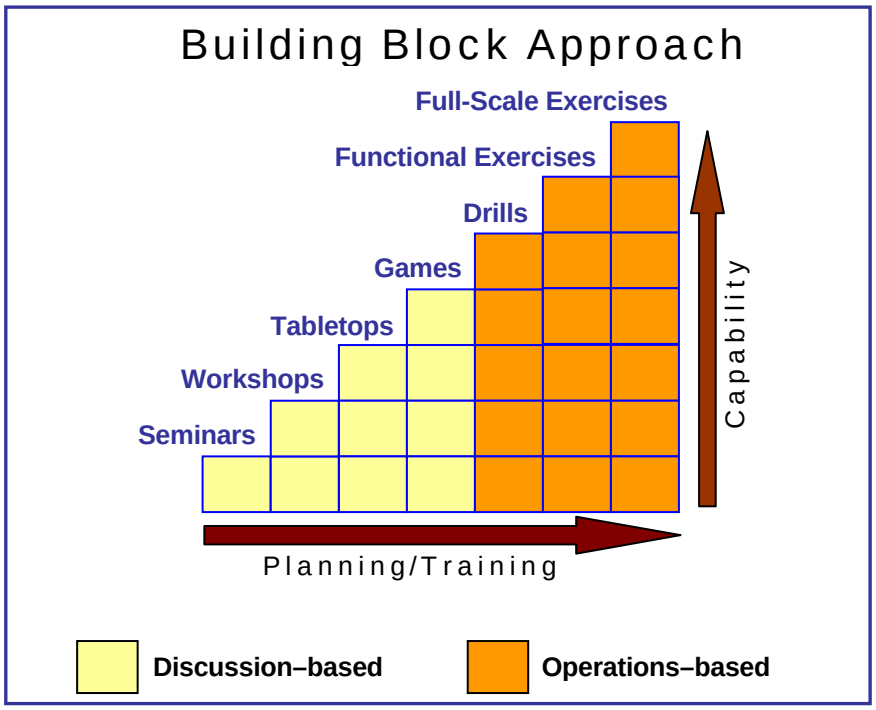
Exercises help the rail transit agency to fulfill these responsibilities. Transit agencies that integrate exercise and evaluation programs into their preparedness activities can more efficiently and effectively execute their emergency response plans during an actual event.

Since the mid-1980s, federal, state and local agencies involved in the design, conduct and evaluation of emergency exercises have emphasized the importance of a progressive exercise program. This approach encourages each rail transit agency to organize and prepare for a series of increasingly complex exercises, using a process where each successive exercise builds upon the previous one to meet specific operational goals. This program is coordinated using a set of project management tools that promote defined goals, measurable objectives, formal schedules, and dedicated resources.

A progressive program implements a cycle of emergency planning, training, exercises, and improvement actions. This cycle is used to direct and schedule exercise activity, and then to ensure that identified improvements are addressed. This program begins with the establishment of a three-year exercise cycle. Within this cycle, targeted areas of focus are then identified based on formal needs assessments, threat and vulnerability assessments, and the recommendations of senior personnel. For example, target areas may include the use of communications equipment and systems across multiple jurisdictions, the integration of rail transit resources into the incident/unified command system established by local responders, and/or the performance of specific types of activities in the rail transit environment (de-energizing and re-energizing third rail or overhead catenary systems, station and vehicle evacuations, or procedures for managing suspicious packages in transportation facilities and on vehicles).

Next, emergency response plans, policies, procedures, immediate actions and job aids are developed or existing documents are reviewed in these focus areas, and training is provided (or the quality of existing training is assessed). Then, over the course of the three-year cycle, increasingly

more complex types of exercises are conducted to assess and reinforce critical activities within the target areas of focus. Each exercise is evaluated, and results are incorporated into the planning development process. As indicated in the figure below, following this "building block" approach, over the three-year cycle, the rail transit agency will conduct seminars, workshops, tabletops, games, drills, functional exercises and, culminate in a full-scale exercise.



To support effective SEPP implementation, the rail transit agency has already developed its *Three-year Exercise Schedule and Program*. Following this schedule, the rail transit agency has already conducted security awareness seminars and workshops and will continue this approach for presenting its revised *Incident Management Organization* and Emergency Operations Plan, as well as basic requirements for NIMS/ICS. The rail transit agency has also conducted a tabletop regarding an Improvised Explosive Device in a rail transit station. Executive Leadership has already participated in "war gaming" conducted by the American Public Transportation Association and co-sponsored by the Transit Cooperative Research Program.

Drills and spot-inspections are routinely conducted by operations and maintenance supervisors to ensure transit personnel knowledge of and compliance with a variety of safety and security-related policies and procedure. The rail transit agency is currently planning and developing both a functional exercise and a full-scale exercise with regional UASI and RTSWG partners, using its newly developed *Incident Management Organization*, and the NIMS and Incident Command models used by regional emergency management and public safety agencies. These two exercises will address (1) the IED prevention and response requirements and the (2) regional CBRNE exercise plan requirements pursuant to HSPD-8 and the Regional Transit Security Strategy.

In 2002, the rail transit agency received an Emergency Preparedness Drills grant from FTA. The purpose of the drills was to exercise the rail transit agency's plans and protocols during a Weapons of Mass Destruction event. A table-top exercise was held in July 2003 involving an unknown

explosive device left in a rails station receiving passengers for a sold out sporting event. A full-scale exercise was held November 2003 involving aerosol dispersal of an unknown substance on a rail vehicle train spraying transit passengers that who had boarded to depart the airport station. Shortly after these exercises, the rail transit agency filed after-action reports with both FTA and the state oversight agency.

The region's Urban Area Security Initiative, Point-of-Contact working group members continually share opportunities for joint exercises. A single, coordinated Urban Area (UA) exercises planning calendar is updated monthly by the members. Additional coordination of the UA's exercise calendar is performed monthly by the technical committee of the UA's Regional Emergency Management Group (REMG), which includes UAPOC members and leaders of UA functional discipline working groups. The rail transit agency, represented on both the UAPOC and REMTEC committees, encourages the UA's responder and emergency management agencies to situate exercises on the transit system whenever possible, for mutual benefit to responder organizations and the transit system.

A highly collaborative culture exists in the regional UA among responder and emergency management agencies, with long-standing support to transit system incidents. As a result, there are ongoing exercises in the regional UA involving the transit system, which at the same time fulfill exercise objectives of the sponsoring responder or emergency management agencies. Examples of these regional drills involving the rail transit agency include: Regional bioterrorism tabletop (sponsored by regional Public Health organizations); Regional earthquake full-scale (sponsored by County Emergency Management Agency); Plane crash full-scale exercise at Municipal Airport (sponsored by the airport); and Multi-agency terrorism explosive tabletop (sponsored by the state Emergency Management Agency).

To support the evaluation of emergency exercises, the rail transit agency has committed to following the methodology specified in G&T's *Homeland Security Exercise and Evaluation Program Volume II: Exercise Evaluation and Improvement.* This volume identifies DHS mission outcomes in support of the National Preparedness Goal, and provides guidelines for preparing an Exercise Evaluation Guide, to provide evaluation and performance measures to be used during rail transit exercises, which assess results in terms of DHS mission outcomes. This volume also provides guidance on developing after action reports compliant with G&T requirements. While the rail transit agency has not yet applied for funding assistances from the DHS Homeland Security Exercise and Evaluation Program, it may do so in the next year.

5.0 Threat and Vulnerability Identification, Assessment, and Resolution

Chapter 5 of the SEPP outlines the rail transit agency's process for managing threats and vulnerabilities during operations, and for major projects, extensions, new vehicles and equipment, including integration with the safety certification process.

Threats are defined as "any real or potential condition that can cause injury or death to passengers or employees of damage to or loss of transit equipment, property, and/or facilities." Threats range from the extreme of CBRNE releases to more common events such as theft of service, pick-pocketing, graffiti and vandalism. **Vulnerabilities** are defined as "characteristics of passengers, employees, vehicles, and/or facilities which increase the probability of a security breach."

Threat and vulnerability assessment provides an analytical process to consider the likelihood that a specific threat will endanger the rail transit system. Threat and vulnerability analysis can also identify activities to be performed to reduce risk of a security threat and mitigate its consequences. Threat and vulnerability assessment methodologies offer rail transit decision makers a consistent and mutually agreed-upon process for addressing security risks.

Given the size and ubiquitous nature of the rail transit network, decision makers cannot possibly protect every element of the transportation infrastructure from every type of security event. Nevertheless, an informed threat and vulnerability assessment process can provide a structured and systematic way to ensure that the rail transit agency receives a maximum level of security for its investment. This process will also focus resources where they are most needed to reduce vulnerabilities with the greatest potential for significant harm in the rail transit network.

Recent events have raised expectations that those entrusted with planning, designing and operating the nation's transportation infrastructure are making adequate provisions to mitigate security risks. As shown in the figure below, DHS/G&T, FTA, FHWA, and a Blue Ribbon Panel of transportation and security experts have also issued guidelines and recommendations which address threat and vulnerability assessment.

Existing Guidelines for Transportation Threat and Vulnerability Assessment

As required by FTA's revised 49 CFR Part 659 and the state oversight agency, in performing the threat and vulnerability assessments to be documented in Chapter 5 of the SEPP, rail transit agencies should, at a minimum, reference the process specified in "Chapter 5: Reducing Threat and Vulnerability" in FTA's *Public Transportation System Security and Emergency Preparedness Planning Guide* (January 2003), available on FTA's safety and security website at: http://transit-safety.volpe.dot.gov.

For those rail transit agencies participating in the DHS G&T Transit Security Grant Program, other practices may be referenced, such as adoption of the threat and vulnerability assessment process specified in G&T's *Special Needs Jurisdiction Tool Kit,* or a process jointly developed by the rail transit agency and G&T as a result of G&T's Technical Assistance Program for Risk Assessment. The G&T program follows an approach similar to what is described in FTA's *Public*

Transportation System Security and Emergency Preparedness Planning Guide, which is a referenced requirement in the DHS Transit Security Grant Program application.

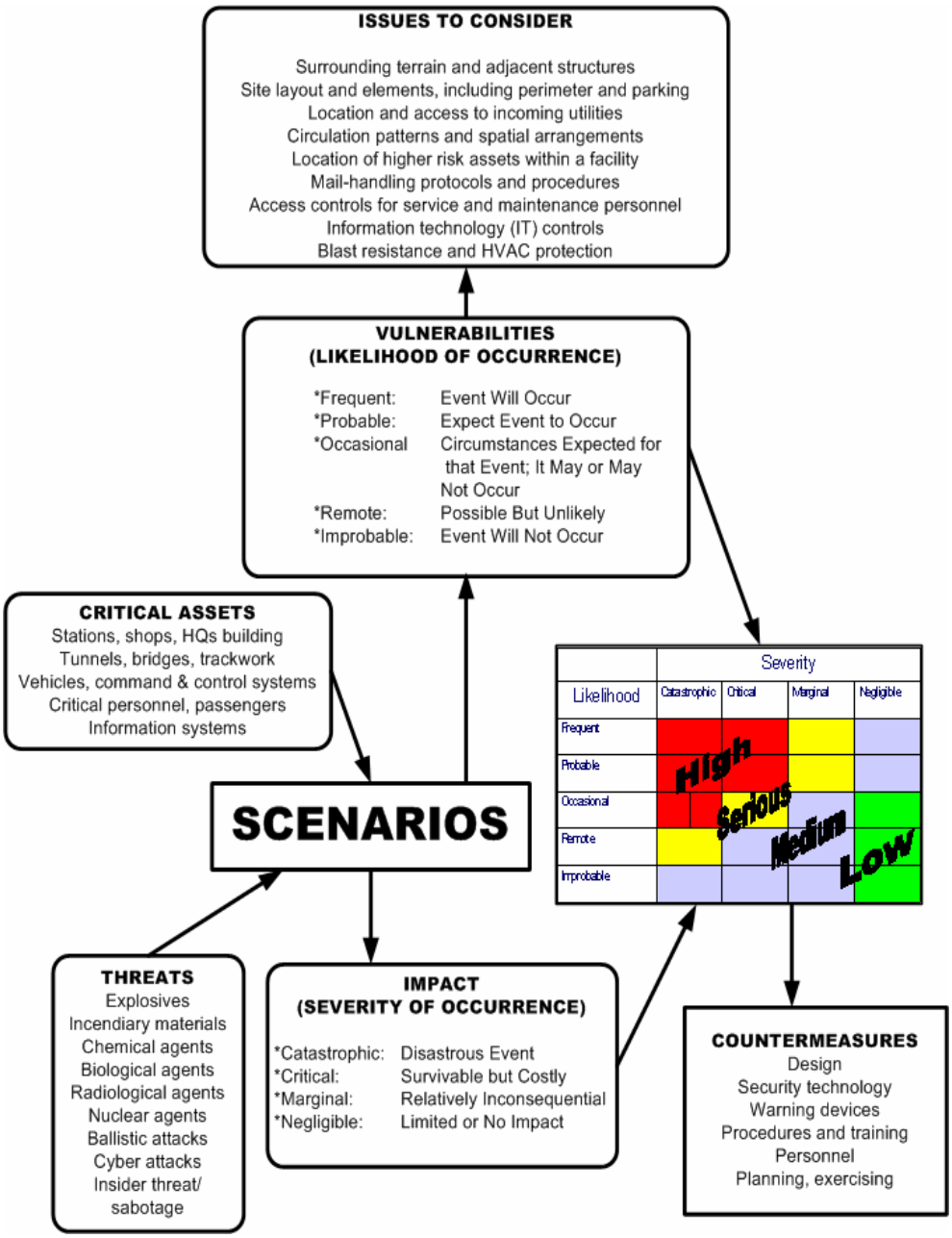
In preparing this SEPP chapter, the rail transit agency should begin by describing the methods the transit system will use to prioritize critical assets and to identify threats and vulnerabilities to those assets. Once threats and vulnerabilities have been systematically identified, they should be assessed to determine their impact on both the affected asset(s) and the entire system, to ensure that the greatest risks to the agency, its passengers and employees are identified. Finally, the process used by the rail transit agency to make decisions regarding whether potential impacts from identified threat and vulnerabilities will be accepted, mitigated or eliminated, should be explained. For each of these activities, the SEPP should also identify the department/function responsible.

In addressing these three elements, FTA's recommended methodology from its *System Security and Emergency Preparedness Planning Guide* is presented graphically in the figure on the next page. The *G&T Special Needs Jurisdiction Risk Assessment Process* is summarized on the page following the figure. In this SEPP chapter, the rail transit agency can describe whichever approach is the most appropriate for its operations and its status in the G&T Transit Security Grant Program.

5.1 THREAT AND VULNERABILITY IDENTIFICATION

- ***Element*:** *Description of the rail transit agency's activities to identify security and terrorism-related threats and vulnerabilities.*

This section of the SEPP should begin by describing the methods the transit system will use to identify security and terrorism-related threats and vulnerabilities. Typically, this process begins with the identification and prioritization of rail transit agency assets. Then, using the rail transit agency's process for security data collection and analysis, specific threats and vulnerabilities are identified for each prioritized asset.



FTA's Threat and Vulnerability Process

G&T Special Needs Jurisdiction Risk Assessment Process	
Steps in Process	**Required Forms**
CRITICALITY ASSESSMENT Step 1—Create an all-inclusive list of candidate critical assets Step 2—Identify and describe critical asset factors Step 3—Assign critical asset factor values Step 4—Apply critical asset factors to candidate critical assets Step 5—Prioritize critical assets **THREAT ASSESSMENT** Step 1—Develop a list of WMD types Step 2—Evaluate the likelihood of weapon use Step 3—Evaluate target attractiveness Step 4—Define scenarios to be used for further analysis **VULNERABILITY ASSESSMENT** Step 1—Assign scenario identifiers Step 2—Identify scenario specifics Step 3—Rate probabilities Step 4—Perform decision tree analysis **IMPACT ASSESSMENT** Step 1—Copy information from previous forms Step 2—Generate Impact ratings Step 3—Calculate overall Impact level **RISK ASSESSMENT** Step 1—Populate risk worksheet Step 2—Determine the vulnerability rating Step 3—Determine the consequence rating Step 4—Plot values on risk diagram Step 5—Analyze risk diagram	Form 1. Critical Asset Factors Worksheet Form 2. Critical Assets Worksheet Form 3. Weapons Matrix Form 4. Target Attractiveness Worksheet Form 5. Scenario Development Worksheet Form 6. Vulnerability Worksheet Form 7. Vulnerability Decision Tree Form 8. Impact Worksheet Form 9. Risk Worksheet Form 10. Relative Risk Diagram Form 11. Capability STEP Process for Scenarios Form 12. Jurisdiction Functional Area Average Scores Form 13. Security Countermeasure/Response Capability Types Form 14. Identification of Measures Form 15. Security Countermeasure/Response Capability Summary Form 16. Security Countermeasure/Response Capability Prioritization Form 17. Needs Consolidation

5.1.1 Asset Analysis

In security terms, assets are broadly defined as people, information, and property. For rail transit agencies, the people typically include passengers, employees, visitors, and contractors, vendors, nearby community members, and others who come into contact with system. Information includes operating and maintenance procedures, vehicle control and power systems, employee information, computer network configurations and passwords, and other proprietary information. The range of rail transit assets that a SEPP program might consider is presented in the table below.

Rail Transit Assets	
▪ Passenger stations, transit centers, and stops ▪ Tenant facilities in passenger stations ▪ Passenger vehicles ▪ Structures (underground, at-grade and elevated) ▪ Passenger parking lots ▪ Vehicle control systems ▪ Communications systems ▪ Heavy maintenance facilities ▪ Service and inspection facilities ▪ Maintenance vehicles and equipment ▪ Backup power systems ▪ Switches, signals and interlockings	▪ Grade crossings and automatic warning devices (gates, bells, flashers, and signs) ▪ Electrification Systems (3rd rail, overhead catenaries) ▪ Operations control centers ▪ Revenue collection facilities ▪ Vehicle storage facilities ▪ Wayside support and maintenance facilities ▪ Ancillary facilities and storage ▪ Employee parking lots ▪ Administrative facilities ▪ Security/police facilities and communications systems

In reviewing assets, the rail transit agency should prioritize which among them has the greatest consequences for people and the ability of the system to sustain service. These assets may require higher or special protection from an attack. In making this determination, the system may wish to consider:

- the value of the asset, including current and replacement value;
- the value of the asset to a potential adversary;
- where the asset is located;
- how, when, and by whom an asset is accessed and used; and
- the impact, if these assets are lost, on passengers, employees, public safety organizations, the general public and the public transportation operation.

There are a variety of worksheets which may be used by the rail transit agency in identifying which assets in their operations would produce the greatest losses to the system and the community. Worksheets are included in the *System Security and Emergency Preparedness Planning Guide*, as well as in the G&T *Special Needs Jurisdiction Risk Assessment* process. G&T's on-site technical assistance program also supports the activities of rail transit agencies in identifying critical assets.

Based on the results of the completed worksheets, the rail transit agency should have a listing of its most important assets. Rail transit agencies participating in G&T programs should share this listing with the Regional Transit Security Working Group and the Urban Area Security Initiative Point-of-Contact Working Group to support regional prioritization of assets and security planning.

Rail transit agency departments/functions responsible for the identification of critical assets typically include the capital/planning department/function, the system safety function, and the security/police function.

5.1.2 Security Data Collection for the Identification of Threats and Vulnerabilities

The rail transit agency's security/police function is often the central point for collection, assessment, reporting and recordkeeping of security data and information involving the rail transit system. The rail transit agency's security database includes standard crime analysis codes, and information sorted by geographic location, geographic area, day of week, time of day, and train route. Analysis of the security database is conducted continually to indicate patterns of criminal behavior occurring on the rail transit system, as a valuable tool used to help determine deployment of security resources on the system. The rail transit agency's security/police function also receives security threat and crime intelligence through law enforcement sources in the region continually and concurrently, for assessment and incorporation into security personnel resource deployments and tactics and rail transit agency operations orders. Security data and information inputs to the security/police function include:

- security incident or breach reports from supervisors, operators, or other personnel;
- security incident or breach reports involving the transit system from local law enforcement agencies in the rail transit system's service area;
- security threat and crime information from law enforcement sources in the region;
- security complaints from citizens and rail transit agency customers;
- special event service plans and information from the rail transit agency's operating and maintenance departments/functions, for assessment of security risks and incorporation of security plans into the overall service plan for the special event;
- security inspections and assessments of transit system facilities and operations performed by the security/police function (in collaboration with the system safety function and representatives of the facility user departments); and
- security-related information from individual rail transit agency employees and through rail transit agency Safety and Security Committees.

In addition, the rail transit agency is a member of the U.S. DOT and APTA-sponsored Surface Transportation Information Sharing and Analysis Center (ST-ISAC), and monitors daily threat information reported by ST-ISAC. The rail transit agency's security/police function is also provided transit-related intelligence information from the regional FBI Joint Terrorism Task Force (JTTF). The rail agency will also join the state-wide terrorism early warning system, when it is operational next year.

Every effort is made to compile all security-related data and reports into the most complete accounting of transit system security information possible. The designated Security Data Coordinator for the security/police function reviews security data and information for accuracy and completeness on an on-going basis, and makes determinations regarding the reliability of the information available as an appropriate basis for security operations and tactics.

5.1.3 Other Sources of Information – Security Reviews, Testing and Inspection Programs

The rail transit agency's threat and vulnerability identification process also includes security testing and inspections. These activities are geared toward ensuring that equipment is operating properly, is readily available when needed, and that employees are proficient in the use of the equipment. To accomplish this, testing programs are developed for specific systems and equipment that not only assess the current state of security, but can also be used to upgrade staff effectiveness through training.

The rail transit agency conducts formal reviews of every incident on its transit system which may require changes in or additions to operating procedures, training programs, or to the design of vehicles, equipment or facilities. Security or emergency incident reviews are generally conducted through the rail transit agency's Security Committee. The rail transit agency's security/police function typically leads the review process for security or emergency incidents. The incident reviews identify causes, and corrective actions, as appropriate.

The rail transit agency has designated employees at each of its operating facilities and office buildings, responsible to coordinate with occupant work groups at each facility and the rail transit agency's security/police function to assure that internal security procedures are identified and followed, and that appropriate physical features and equipment for building/site security are identified, implemented and maintained at each work facility. At a typical operations facility, the security representatives are the maintenance and transportation operations managers of that location. In addition, monthly safety inspections of operating facilities, which are performed by these personnel, include inspections of security-related items. Managers responsible for maintenance of the respective facilities are responsible to correct any security items found non-compliant by the monthly safety/security inspections.

The rail transit agency security/police function also supports facility security representatives and operations managers by providing security assessments of transit system assets such as transit centers, park/ride facilities, light rail tunnel and stations, and operations facilities. Supplemental or update assessments may occur whenever prompted by identification of a vulnerability or in corrective action resulting from a security breach incident review.

Within the security/police function, security data and information is processed in three (3) functional areas:

- the Security Data Coordinator continually collects, analyzes and reports data related to transit crime and security incidents, and maintains the agency's security information database;
- officers in the security/police function provide continuous identification and assessment of transit system security threats and vulnerabilities; and
- management staff in the security/police function continually translates incoming information into security plans and operations orders for personnel deployment, tactical operations, missions, investigations, and coordination of activities with rail transit agency operating departments/functions and operations of local jurisdiction law enforcement agencies.

Security data and information outputs from the security/police function include:

- transit crime data is reported monthly to FTA's National Transit Database, and to the state safety oversight agency;
- detailed reports provided during monthly Security Coordination Team meetings, including transit crime data reports and trend analysis, security incident reviews and recommendations, security plans for special event transit service or regional events affecting the transit system, facility security assessments, and security program recommendations; and
- reports from security inspections and assessments of transit system facilities.

In addition, the Operations Control Center reports rail transit security incidents meeting specified thresholds to the state oversight agency, as required in 49 CFR Part 659. Every effort is made to issue these reports within two-hours of incident occurrence, as per the standard of 49 CFR § 659.33. Full investigations are conducted of these events, and corrective action plans are developed, reviewed and approved by the state oversight agency, and tracked through to implementation by the security/police function.

As security issues are identified, they are documented and addressed through security design criteria; development of new procedures and practices; employee training; changes in the deployment of security personnel; and targeted integration with relevant local law enforcement and regional emergency management agencies. The security/police function takes the lead in coordinating rail transit agency activity to address the results of security information collection.

5.1.4 Identifying Threats for Prioritized Assets

Based on this security information collection and analysis process described above, the rail transit agency will identify specific threats for its list of prioritized assets. This activity is termed “threat analysis.” Threat analysis defines the level or degree of the threats against a prioritized asset by evaluating the intent, motivation, and possible tactics of those who may carry them out. The process involves gathering historical data about the ways in which criminals have perpetrated crimes on the systems and also, for terrorism, identifying ways in which threats could be carried out again the system. In performing this assessment, the rail transit agency should identify and evaluate which information, from all that is collected, is relevant in assessing the threats against the prioritized assets. This activity may be performed by the security/police function with the support of a consultant and the system safety function.

Specifically for terrorism, possible methods of carrying out hostile actions in the transportation environment are depicted in the table on the next page. Historical examples are provided for reference and consideration, as well as the types of weapons typically used in these attacks.

Potential Threats from Terrorism

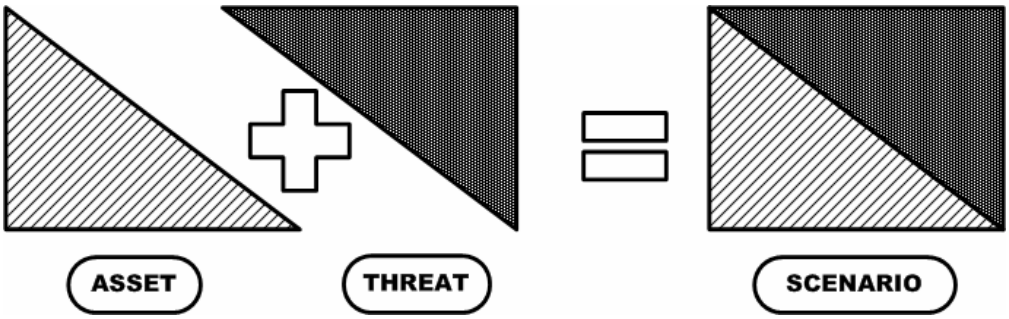
Type of Attack	Historical Example	Type of Weapons
Explosive and Incendiary Devices	2005 London Underground and Bus Bombings 2004 Madrid Bombings 1995 GIA bombing of Paris Metro	Planted Devices
	HAMAS suicide bombs on Israeli buses (on-going)	Suicide Bombs
	1998 bombings of U.S. Embassies in Tanzania and Kenya	Vehicle Bomb
	2001 World Trade Center 1990s abortion clinic bombings in GA 1995 Oklahoma City Bombing	Proximity Bombs; Incendiary Devices; Secondary Devices
Exterior Attacks	2001 militant assaults on Indian-held mosques in Kashmir	Rocks and Clubs; Improvised Devices; Molotov cocktails
Stand-off Attacks	Tamil Tiger's July 2001 mortar attack & bombing of Sri Lanka's National Airport	Anti-tank rockets; Mortars
Ballistics Attacks	Long Island Railroad Shootings; Columbine High School	Pistols; Handguns; Submachine guns; Shotguns
Networked/ Inside Access: - Forced Entry - Covert Entry - Insider Compromise - Visual Surveillance - Acoustic/ Electronic Surveillance	Amtrak *Sunset Limited* derailment 1996 Tupac Amaru Revolutionary Movement taking of Japanese Ambassador's residence and 500 guests in Peru (access through disguise as waiters at the party)	Hand, power and thermal tools; Explosives
		False credentials; Stolen uniforms and identification badges
		False pretenses, cell operations
		Binoculars; Photographic Devices
		Listening Devices; Electronic-emanation surveillance equipment
Cyber Attack	Code Red Worm (2002)	Worms, Viruses, Denial of Service Programs
Chemical, Biological, Radiological, & Nuclear (CBRN) Agent Release	1995 Aum Shinrikyo Sarin Gas Release in Tokyo Subway	Chemical, biological, or radiological or nuclear aerosolized

Identified threats for each prioritized asset may be recorded in worksheets or databases are maintained by the rail transit agency's security/police function. Sample worksheets are included in the *System Security and Emergency Preparedness Planning Guide*, as well as in the G&T *Special Needs Jurisdiction Risk Assessment* process.

5.1.5 Identifying Vulnerabilities

A vulnerability is anything that can be taken advantage of to carry out a threat. This includes vulnerabilities in the design and construction of a facility, in its technological systems, and in the

way a facility is operated (e.g., security procedures and practices or administrative and management controls). To identify vulnerabilities, the rail transit agency should pair prioritized assets with identified threats to create scenarios. This activity is termed "vulnerability analysis."



Vulnerability analysis identifies specific weaknesses with respect to how they may invite and permit a threat to be accomplished. Vulnerabilities are commonly prioritized through the creation of scenarios that pair identified assets and threats. Using these scenarios, transportation agencies can evaluate the effectiveness of their current policies, procedures, and physical protection capabilities to address consequences.

In conducting its vulnerability analysis, the rail transit agency should apply an interpretive methodology that encourages role-playing by transportation personnel, emergency responders, and contractors to brainstorm ways to attack the system. By matching threats to critical assets, transportation personnel can identify the capabilities required to support specific types of attacks. This activity promotes awareness and highlights those activities that can be preformed to recognize, prevent, and mitigate the consequences of attacks.

Both the FBI and DHS recommend that rail transit agencies focus on the top 10% of identified critical assets (at a minimum). Using these assets, transportation personnel should investigate the most likely threats, considering the range of attack objectives and methods that may be used (such as property and violent crime, disruption of traffic, destruction of bridge or tunnel, airborne contamination, hazardous materials accident, and threat or attack with explosives intended to disrupt or destroy). The system should also consider the range of perpetrators, such as juvenile gang members, drug users and pushers, car thieves, organized crime, terrorists, disgruntled employees, disturbed copycats, and others.

When conducting the scenario analysis, the system may choose to create chronological scenarios (event horizons) that emphasize the worst credible scenario as opposed to the worse case scenario. Experienced transportation personnel, who have participated in transportation war-gaming, recommend the investigation of worst credible scenarios. Based on this type of assessment, as indicated in the table, the rail transit system may determine certain scenarios as the most relevant. Results can be recorded in worksheets provided in *System Security and Emergency Preparedness Planning Guide*, as well as in the G&T *Special Needs Jurisdiction Risk Assessment* process.

Relevant Rail Scenarios

Rail Assets	Most Probable Threats
Stations	▪ High-yield vehicle bomb near stations ▪ Lower-yield explosive device in station ▪ Armed assault, hijacking, hostage, or barricade situation in station ▪ Chemical, biological, and nuclear release in station ▪ Secondary explosive device directed at emergency responders ▪ Graffiti in station ▪ Car theft from station parking lot
Track/signal	▪ Explosive detonated on track ▪ Chemical, biological, nuclear release on track ▪ Signal and/or rail tampering ▪ Dumping of debris on track
Rail cars	▪ Explosives placed on or under rail car ▪ Improvised explosive device (pipe/fire bomb) on rail car ▪ Chemical, biological, nuclear release on rail car ▪ Armed assault, hostage, or barricade situation on rail car ▪ Secondary explosive device directed at emergency responders ▪ Graffiti on rail car
Power substations	▪ Explosive detonated in or near substation ▪ Tampering with power substations and components
Command Control Centers	▪ Physical or information attack on train control system ▪ Physical or information attack dispatch system ▪ Armed assault, hostage, or barricade situation ▪ Explosive device near or in Center ▪ Sabotage of train control system

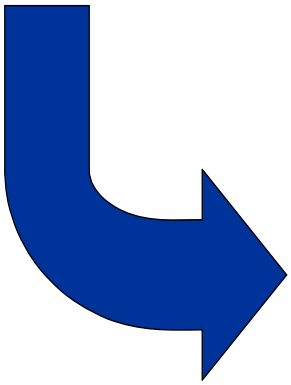
5.2 THREAT AND VULNERABILITY ASSESSMENT

- ***Element*:** *Description of the rail transit agency's activities to assess the likely impacts of identified threats and vulnerabilities on the system and to identify particular vulnerabilities which require resolution.*

Threats and vulnerabilities to a transit system cover a wide array of events, virtually none of which can be totally eliminated while still operating the system. Since no system can be rendered totally secure, once threats and vulnerabilities are identified, their impact on the total system must be assessed to determine whether to accept the risk of a particular danger, and the extent to which corrective measures can eliminate or reduce its severity.

To conduct its threat and vulnerability assessment, for each scenario pairing prioritized assets with identified threats, the transportation system should attempt to identify the costs and impacts using a standard risk level matrix, which supports the organization of consequences into categories of high, serious, and low. Consequences are assessed both in terms of severity of impact and probability of loss for a given threat scenario. A sample matrix is presented below:

	Vulnerability	Impact	
Very Easy	A	I	Loss of life
Relatively Easy	B	II	Serious injuries, major service impact, >$250k damage
Difficult	C	III	Minor injuries, minor service impact, <$250k damage
Very Difficult	D	IV	No injuries, no service impact
Too Difficult	E		



Criticality Matrix

	I	II	III	IV
A	H	H	S	S
B	H	H	S	L
C	H	S	L	L
D	S	L	L	L
E	S	L	L	L

- H = High
- S = Serious
- L = Low

Sample Threat and Vulnerability Assessment Matrix

Scenarios with vulnerabilities identified as "high" may require further investigation and the implementation of countermeasures. Scenario-based analysis is not an exact science but rather an illustrative tool demonstrating potential consequences associated with low-probability to high-impact events. To determine the system's actual need for additional counter-measures, and to provide the rationale for allocating resources to these counter-measures, the system should use the scenarios to pin-point the vulnerable elements of the critical assets and make evaluations concerning the adequacy of current levels of protection.

Examples of vulnerabilities that may be identified from scenario-based analysis include the following:

- accessibility of surrounding terrain and adjacent structures to unauthorized access (both human and vehicular);
- site layout and elements, including perimeter and parking that discourage access control, support forced or covert entry, and support strategic placement of explosives for maximum damage;
- location and access to incoming utilities (easy access for offenders);

- building construction with respect to blast resistance (tendency toward progressive collapse, fragmentation, or no redundancy in load bearing);
- sufficiency of lighting, locking controls, access controls, alarm systems, and venting systems to support facility control; and
- information technology (IT) and network ease-of-penetration.

At the conclusion of the scenario-based analysis, the transportation system should have assembled a list of prioritized vulnerabilities for its top 10% critical assets. Typically, these vulnerabilities may be organized into the following categories:

- lack of planning;
- lack of coordination with local emergency responders;
- lack of training and exercising; and
- lack of physical security (access control, surveillance; blast mitigation, or chemical, biological, or radioactive agent protection).

These vulnerabilities should be documented in a confidential report or memorandum for the system's executive director. Results can be recorded in worksheets provided in *System Security and Emergency Preparedness Planning Guide*, as well as in the G&T *Special Needs Jurisdiction Risk Assessment* process.

5.3 THREAT AND VULNERABILITY RESOLUTION

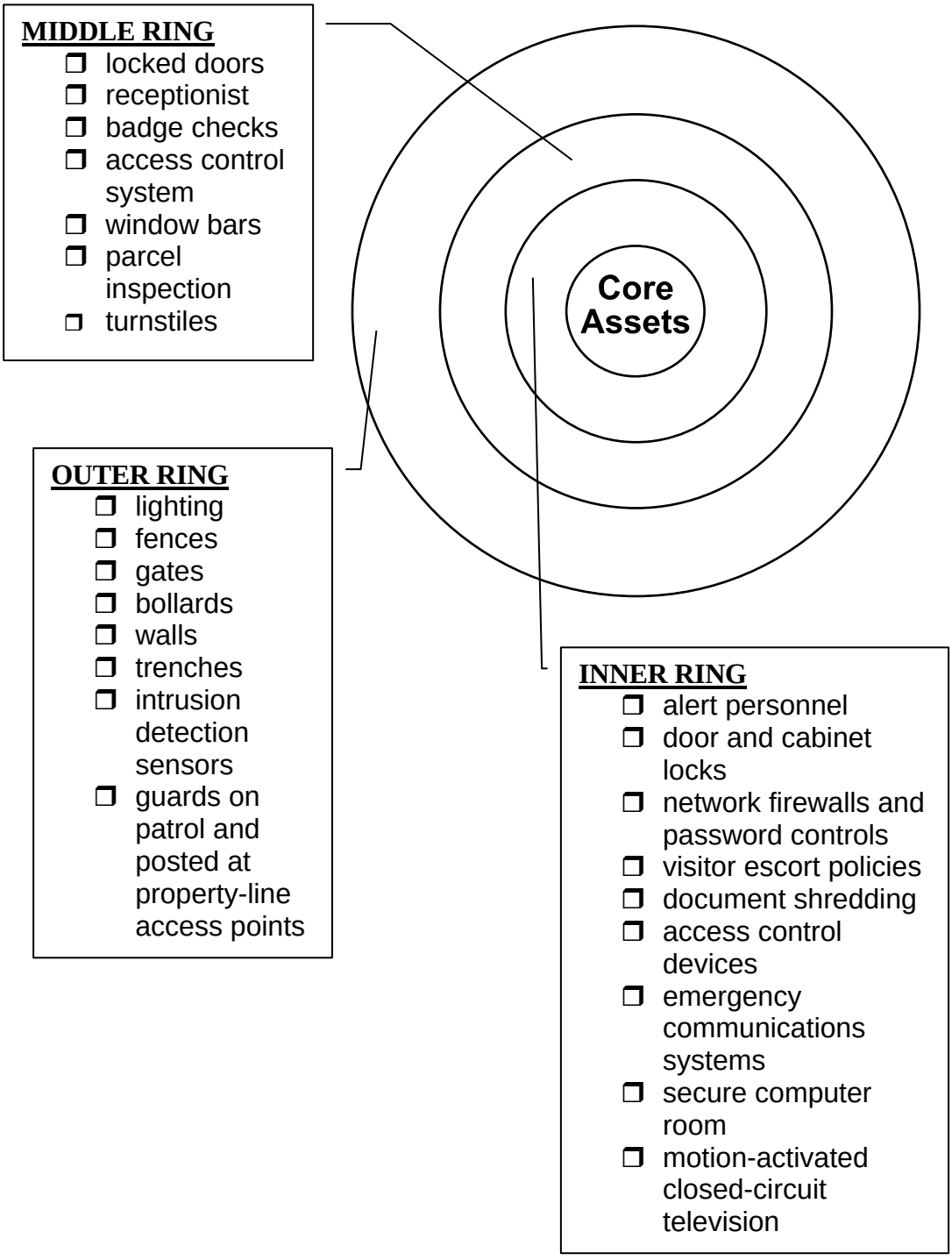
- ***Element:*** *Description of how response strategies (both short- or long-term strategies) are developed for prioritized vulnerabilities, including the decision process used to determine whether to eliminate, mitigate, or accept security problems.*

Based on the results of the analysis described in Section 5.2 of this SEPP, the rail transit system can then identify countermeasures to reduce vulnerabilities identified as unacceptable to management. Effective countermeasures typically integrate mutually supporting elements.

- Physical protective measures designed to reduce system asset vulnerability to crime, explosives, ballistics attacks, cyber attacks, and the release of CBRNE agents.
- Procedural security measures, including procedures to detect and mitigate an act of crime, terrorism, or extreme violence, and those procedures employed in response to an incident that does occur.

As illustrated in the figure on the next page, security tends to emphasize "rings of protection," meaning that the most important or most vulnerable assets should be placed in the center of concentric levels of increasingly stringent security measures. For example, a rail transit agency's Operational Control Center should not be placed right next to the building's reception area, rather, it should be located deeper within the building so that, to reach the control center, an intruder would have to penetrate numerous rings of protection, such as a fence at the property line, a locked

exterior door, an alert receptionist, an elevator with key-controlled floor buttons, or a locked door to the control room.



Sample Rings of Protection

Within the rings of protection concept, the development of countermeasures typically reflects standard precedence guidelines for hazard resolution, including:

- design to eliminate or reduce threats and vulnerability;
- security devices to reduce vulnerability;
- detection/alarm devices for security response; and
- security personnel, and security and emergency procedures and training for all personnel.

As a first step in assessing the need for countermeasures, the rail transit agency assures that the security policies, procedures, responsibilities, equipment, technology, and response capabilities described throughout this SEPP are effectively in-place for all threats, so that the risks of loss from security incidents to transit customers and employees, and to operating performance of the transit system, is at a manageable or acceptable level.

Next, based on the assessment of identified vulnerabilities, the rail transit agency may consider implementation of additional strategies to mitigate or eliminate vulnerabilities. Typically, rail transit agencies consider both passive and active strategies for identifying, managing, and resolving threats to the system's operation. Passive strategies include all security and emergency response planning activity, outreach with local law enforcement, training, evacuation and business continuity and recovery plans, employee awareness, public information, and passenger training. Passive responses also include security design strategies, supported by Crime Prevention Through Environmental Design (CPTED) and Situational Crime Prevention (SCP) methods, such as landscaping, lighting, and physical barriers (planters or bollards).

Active strategies include security technology, such electronic access control, intrusion detection, closed circuit TV, digital recorders, emergency communications systems, and chemical agent or portable explosives detectors. Active systems also include personnel deployment. It is important to consider the entire lifecycle cost when evaluating security solutions. Technology options may require a substantial one-time investment, supported by fractional annual allocations for maintenance and vendor support contracts. Personnel solutions are generally more expensive.

Examples of ways in which the above prioritization may be applied include:

- consideration of resources/action to resolve a potential security threat;
- consideration of a corrective action as part of an security incident review, following a breach; and
- consideration of a CPTED proposal/investment during design development of a transit facility project.

Other prevention strategies involve cooperation with law enforcement agencies, security staff in other systems, and industry associations in order to share threat information. It is useful to know whether other transportation systems in an area have experienced threats, stolen uniforms or keys, or a particular type of criminal activity, in order to implement appropriate security measures.

The table below provides a sample listing of possible countermeasures.

Rail Transit Agency Countermeasures	Planning	Coordination with Local Responders	Training and Exercising	Physical Security			
				Access Control	Surveillance	Blast Mitigation	WMD Agent Protection
Identifying Unusual or Out-of-Place Activity	X		X	X	X		X
Security Screening and Inspection Procedures	X	X	X		X	X	X
Enhancing Access Control for Stations/Vehicles	X	X	X	X		X	
Securing Perimeters for Non-revenue Areas	X			X	X		
Denying Access to Authorized-only Areas	X		X	X	X		
Securing Vulnerable Areas (target hardening)	X			X	X	X	
Removing Obstacles to Clear Line-of-Sight	X			X	X		
Protecting Parking Lots	X			X	X		
Enhanced Access Control for Control Center	X			X	X		
Securing Critical Functions and Back-ups	X			X	X		
Promoting Visibility of Uniformed Staff	X			X	X		
Removing Spaces that Permit Concealment	X			X	X		X
Reinforcing Natural Surveillance	X			X	X		
Procedures for Vehicle and Station Evacuations	X	X	X			X	X
Coordination with Community Planning Efforts	X	X	X				X
Backing up Critical Computer Systems	X		X				
Revising Lost-and-Found Policies	X		X				X
Securing Tunnels and Elevated Structures	X		X	X	X	X	X
Elevating/securing Fresh Air Intakes	X			X			X
Protecting Incoming Utilities	X			X	X	X	X
Establishing Mail-handling Procedures	X		X		X		X
Identifying Appropriate Personal Protective Equipment and Training	X	X	X				X
Preparing Response Folders and Notebooks for Facilities and Vehicles	X	X	X		X	X	X
Familiarization Training for Local Emergency Response Agencies	X	X					X
Planning for Scene Management and Emergency Response	X	X				X	X

Possible Rail Transit Agency Countermeasures

6.0 Implementation and Evaluation of SEPP

6.1 Implementation Tasks for Goals and Objectives

- ***Element:*** *Identification of tasks to be performed to implement the goals and supporting objectives required to implement the SEPP.*

This section should describe the specific tasks that will be implemented by the rail transit agency to meet the goals and objectives specified in Section 1.2 of the SEPP, and the roles, responsibilities and program implementation activities described in the other chapters. For example, for the sample goals and objectives identified in Section 1.2 of this SEPP, the rail transit agency may identify the following tasks:

- Base routine deployment and tactics of transit system security personnel on current intelligence and analysis of crime incidence, trends and threats on the transit system.
- Specialize deployment and tactics of transit system security personnel for special event transit operations, based on intelligence and analysis of crime incidence, trends and threats particular to each special event.
- Frequently deploy transit system security personnel in special missions and tactics to target unfavorable trends in crime or threats on the transit system, identified by crime analysis and intelligence.
- Fulfill perceived security and order issues on the transit system with deployments and tactics of security personnel which enhance visibility to system ridership and stakeholders, and provide an environment in which the rail transit agency's Code of Conduct, regulations and laws of the community are enforced.
- Communicate the System Security Policy and Security and Emergency Preparedness Program, to all personnel.
- Incorporate the security and emergency preparedness responsibilities specific to each employee's job into the training program, procedures and instructions applicable to each job.
- Include security program considerations in performance evaluations of managers according to their respective security program job responsibilities.
- Integrate transit system security procedures, drills/demonstrations, and incident reviews into transportation, maintenance, and safety operating and emergency procedures, drills/demonstrations, and incident reviews.
- Involve employees in security program development and implementation, through mechanisms such as including security considerations in Safety Committees and facility safety inspections, and designating security representatives for each operating facility.
- Reinforce an organizational culture for security responsibility, by enforcing access to transit facilities by authorized personnel only.

- Assure that "Be Alert" and "Transit Watch" notifications are posted in all rail vehicles, transit centers, rail stations, and are included in routine customer information materials such as service brochures and website information.
- Conduct accurate and complete data collection and analysis for all crime and security breaches on the transit system.
- Optimize security personnel deployments and tactics based on continuous crime analysis and threat intelligence.
- Through inter-agency cooperation, assure that all security threat and crime intelligence available in the region significant to the transit system is concurrently available to rail transit agency security/police function for assessment and incorporation into transit system security resource deployments and tactics.
- Provide sufficient personnel and equipment and sufficient levels of security training, to reduce the rate of crime, and the fear of crime, on the system, and to resolve transit system threats and vulnerabilities to acceptable risk.
- Monitor developments in security technologies, and maintain and deploy security equipment so as to optimize effectiveness of system security human resources.
- Provide a level of fare enforcement, and enforcement of the rail transit agency's prohibited conduct regulations, on the system, for high effectiveness in both collection of revenue, and in sustaining public perception that the transit system is reasonably secure from prohibited conduct.
- Perform fare inspections at a rate not less than 3,750 monthly per Fare Inspector.
- Promote inter-agency cooperation and mutual security tactics and operations for the transit system through intergovernmental agreements establishing the rail transit agency security/police function as an extension of local jurisdiction law enforcement and vice-versa.
- Incorporate CPTED guidelines and FTA's Transit Security Design Considerations into rail transit facilities design criteria and design reviews.
- As funds allow, deploy security equipment systems to increase prevention and detection capabilities, including surveillance, access control, and intrusion detection, in priority of risk reduction to assets by criticality.
- Develop partnerships with community organizations which help foster security on the transit system.
- Develop engagements of community-based personnel and services which can cost-effectively contribute to perceived security on the transit system.
- Collaborate development of criminal statutes in the community which benefit the transit system, as well as criminal statutes specific to the transit system, through intergovernmental cooperation, assisted by the rail transit agency's legal function.
- Review the system security program on an on-going basis for performance of its objectives and tasks.
- Update the SEPP annually.

- Complete development and implementation of rail transit agency's Emergency Operations Plan, to reflect integration with the municipal/county Emergency Operations Plan and the Regional Transit Security Strategy (RTSS).
- Per DHS/G&T directives pursuant to HSPD-5, and the Urban Area Regional Transit Security Strategy (RTSS), implement NIMS-compliant ICS at the rail transit agency.
- Per DHS/G&T directives pursuant to HSPD-8, and the UA RTSS, assure that the UA's CBRNE plan development, to be completed by May 1, 2006, incorporates POETE covering potential CBRNE events occurring on the transit system, with priority on potential IED events on mass transit.
- Assure that the rail transit agency is an integral participant in the UA's IED scenario full-scale exercise and in the region's future CBRNE exercises.
- Per DHS/G&T directives pursuant to HSPD-8, the UA RTSS, and recommendations of internal, FTA and G&T-assisted security needs assessments, complete assessment of the rail transit agency's communications and operations control systems needs, coordinated with the UA's communications interoperability plan.
- Assure appropriate involvement of the rail transit agency in planning for, and participation in, DHS-sponsored exercises occurring in the UA.

6.2 IMPLEMENTATION SCHEDULE

- ***Element:*** *General schedule with specific milestones for implementation of the security program, threat and vulnerability analyses, staff security training, and regular program reviews during the implementation process.*

This section should detail a schedule that is used for the implementation of the security program. For example, if the security plan is to be reviewed by the transit agency on an annual basis, beginning in January of each year, then this review should be included in the general schedule. In addition, if specific threat and vulnerability analysis of key stations or facilities are to be updated every year, this section should include those items in the schedule.

6.3 EVALUATION

- ***Element:*** *Description of the types of internal management reviews to be conducted, the frequencies of the reviews, and the person(s) responsible.*

This section of the SEPP should document the rail transit agency's process for conducting internal security audits to evaluate compliance and measure the effectiveness of the SEPP. This process must ensure that all elements in the rail transit SEPP are reviewed for their implementation and effectiveness in an on-going manner over a three-year cycle. This process may be combined with the internal audit process used for the System Safety Program Plan, or it may be an independent procedure.

This section of the SEPP should identify the department/function with responsibility for conducting these audits, the activities to be performed, including establishing the audit schedule,

the development of checklists to guide the audit, and the notification of the state oversight agency no less than 30 days prior to the conduct of an audit, the frequency of the audits, and, if possible, the specific person or internal function responsible. For example, the system safety function may audit the security/police function as part of its internal audit program on a three year basis. In addition, security management may perform weekly or daily reviews of the private security forces it has hired to provide security at transit agency facilities. The rail transit agency must submit an annual report to the state oversight agency for review and approval, documenting its internal audit activities over the past year, along with a certification, signed by the General Manager that, based on the results of internal audit process, the SEPP is being implemented by the rail transit agency.

Any external reviews of the security program should also be explained in this section. The SEPP should state that the state safety oversight agency will conduct an external review of the rail transit agency's SEPP program on a three year basis at a minimum. The transit agency should also explain the process for correcting any findings that are a result of the external review. To respond to findings of an oversight agency external review, the rail transit agency may need to submit a corrective action plan describing how the finding will be resolved. The corrective action plan should include the corrective action plan required, the person(s) or department responsible for implementing the corrective action, a time frame for implementing the corrective action, and the status of the corrective action plan. As applicable, the rail transit agency should also note reviews to be conducted by G&T and/or TSA.

7.0 Modification of System Security Plan

7.1 INITIATION

- ***Element:*** *Description of process used to initiate revisions to the security plan, gather input for the revisions, procedures for updating the security plan, and identification of responsible person(s).*

This section of the SEPP plan should include a process for initiating revisions, gathering input for the revisions and procedures for updating the plan and the identification of the responsible person.

7.2 REVIEW PROCESS

- ***Element:*** *Description of the process used to review and revise the security plan as necessary, including frequency of reviews, and responsible person(s).*

The process used to review and revise the security plans as necessary should be explained, including frequency and responsible person(s). The role of the state safety oversight in requiring annual updates and reviewing the security plan needs to be included in this section.

This section of the SEPP should also document the rail transit agency's process for making its SEPP and accompanying procedures available to the oversight agency for review and approval. As specified in § 659.11 of the revised Rule, the oversight agency must either have provisions in place for protecting security-related materials from public disclosure or the rail transit agency must develop special procedures to ensure that these materials cannot be released. The rail transit

agency's SEPP must describe the process in place to ensure that all security-related materials are protected from public disclosure. In many instances, this may include the state oversight agency conducting an on-site review of the SEPP and supporting procedures at the rail transit by agency.

7.3 IMPLEMENT MODIFICATIONS

- ***Element:*** *Description of process used to communicate and disseminate new and revised procedures and other elements of the security plan to appropriate transit agency staff.*

The process of communicating, disseminating and implementing new and revised procedures of the security plan throughout the transit agency should be detailed.

Appendix A: DHS Regulation and Requirements Relevant to the SEPP

As discussed briefly in Section 1.6 (Government Involvement) and Section 3.3.6 (Responsibilities of External Agencies), DHS and its departments (including G&T, FEMA, and TSA) all have a new role in public transportation system security and emergency preparedness. This section of the SEPP describes the various elements of this role, which are based in the Homeland Security Act of 2002 and subsequent Homeland Security Presidential Directives (HSPDs), and identifies the implications for the rail transit agency.

The authority of the Department of Homeland Security to regulate the security and emergency preparedness operations of public transportation agencies is two-fold. First, DHS has direct regulatory authority over all modes of transportation. See Aviation and Transportation Security Act of 2001, PL 107-71, 115 Stat. 597, 49 USC 40101 (transferring regulation of all modes of security to the Transportation Security Administration (TSA), still within the Department of Transportation) and Homeland Security Act of 2002, PL 107-296, 116 Stat. 2135, 6 USCA 101 (transferring TSA from the DOT to DHS). Thus, DHS (through TSA) has the authority to regulate and oversee implementation of security and emergency preparedness measures for all modes of transportation in the United States. TSA may exercise its authority through formal rulemaking or binding directives to transportation operators. See 49 CFR § 1500–1699 (current rules as codified).

Second, DHS has control over the intergovernmental coordination of national security operations, and because public transportation agencies are "local governments" as defined in the Homeland Security Act, they are subject to the guidelines and any grant-based requirements associated with DHS coordination efforts. See Homeland Security Act of 2002, PL 107-296, 116 Stat. 2135, 6 USCA 101. The Office of the Secretary of DHS includes the Office of State and Local Government Coordination and Preparedness (SLGCP), which includes G&T, which plays a major role administering and managing DHS grant programs. FEMA, now a part of DHS, also plays a significant role in coordinating intergovernmental activities for all-hazards emergency preparedness.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVES AND SUPPORTING GUIDANCE

Under the Homeland Security Act, activities identified to support intergovernmental coordination are carried out primarily by G&T and FEMA, following guidance and requirements specified in Homeland Security Presidential Directives (HSPDs), particularly:

Homeland Security Presidential Directive 5: Management of Domestic Incidents, February 28, 2003

- National Incident Management System (NIMS) - March 2004
- National Response Plan - December 2004

Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003

- National Infrastructure Protection Plan (NIPP) - (interim) February 2005

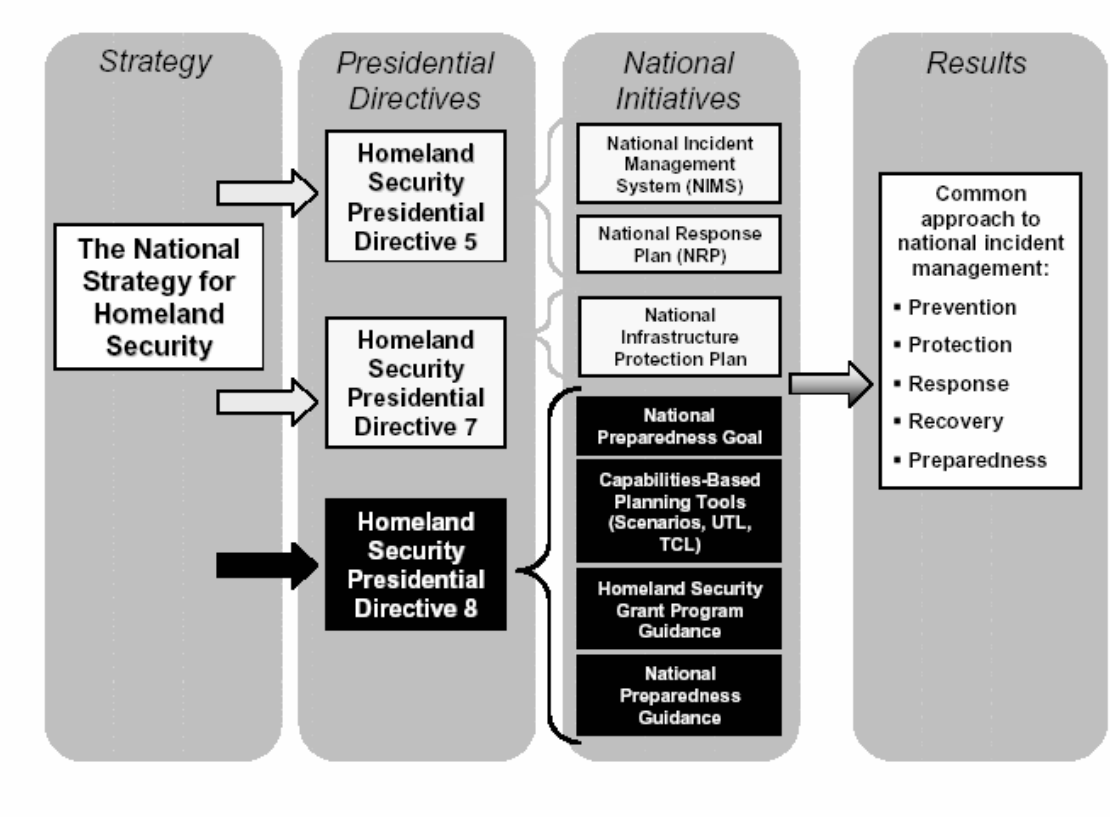
Homeland Security Presidential Directive 8: National Preparedness, December 17, 2003

- National Planning Scenarios - August 2004

- National Preparedness Goal - draft March 2005
- Universal Task List - December 2004 (v.2)
- Target Capabilities List - February 2005
- Homeland Security Grant Program Guidance - December 2004
- National Preparedness Guidance - April 2005
- DHS/G&T Transit Security Grant Program Guidance - April 2005
- State and Urban Area Homeland Security Strategy Guidance on Aligning Strategies with the National Preparedness Goal, July 2005

Relationships among HSPDs 5, 7 and 8 are depicted graphically in the figure below.

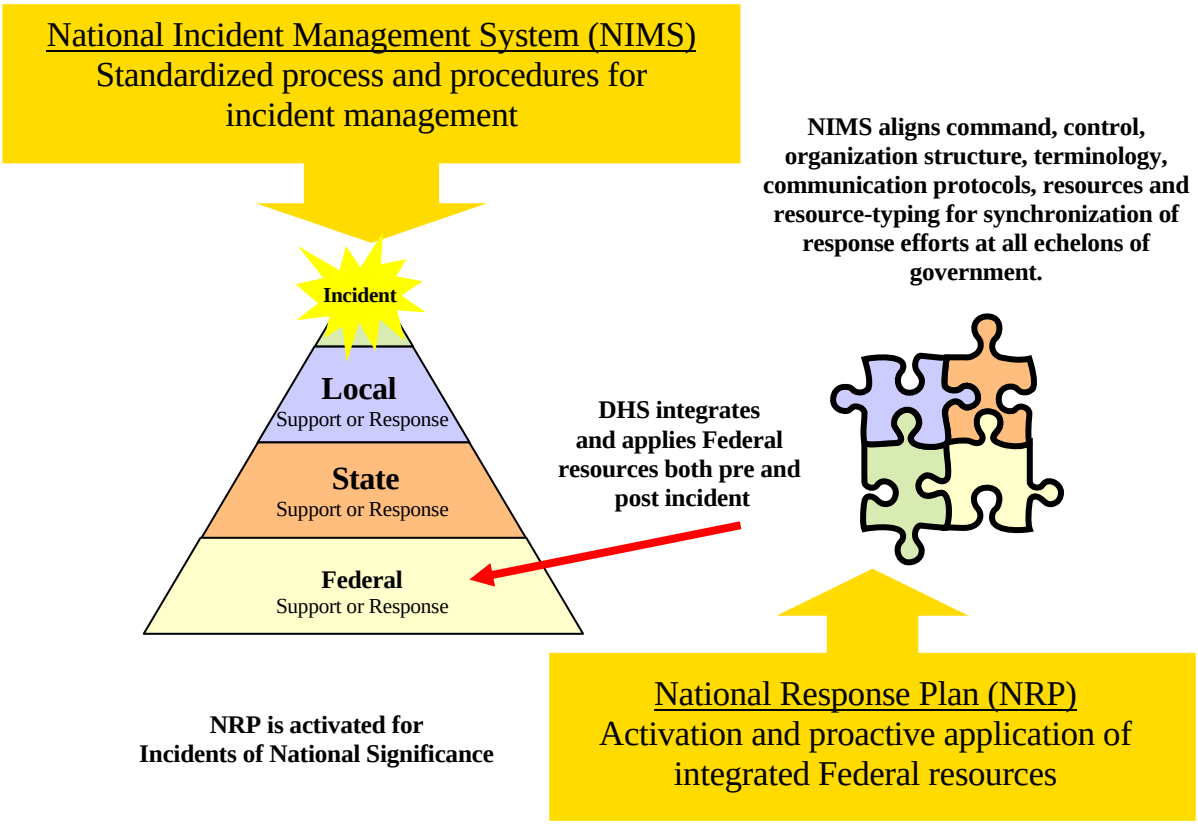
DHS Strategy, HSPDs, National Initiatives and Expected Results



HSPD-5 (Management of Domestic Incidents) mandated the creation of the National Incident Management System (NIMS) and National Response Plan (NRP). The NIMS provides a consistent framework for entities at all jurisdictional levels to work together to manage domestic incidents, regardless of cause, size, or complexity. To promote interoperability and compatibility among federal, state, local, and tribal capabilities, the NIMS includes a core set of guidelines, standards, and protocols for command and management, preparedness, resource management, communications and information management, supporting technologies, and management and maintenance of NIMS. The NRP, using the template established by the NIMS, is an all-discipline, all-hazards plan that provides the structure and mechanisms to coordinate operations for evolving or potential Incidents of National Significance. Incidents of National Significance are major events that "require a coordinated and effective response by an appropriate combination of federal, state,

local, tribal, private sector, and nongovernmental entities." The relationship of NIMS and the NRP during Incidents of National Significance is presented below.

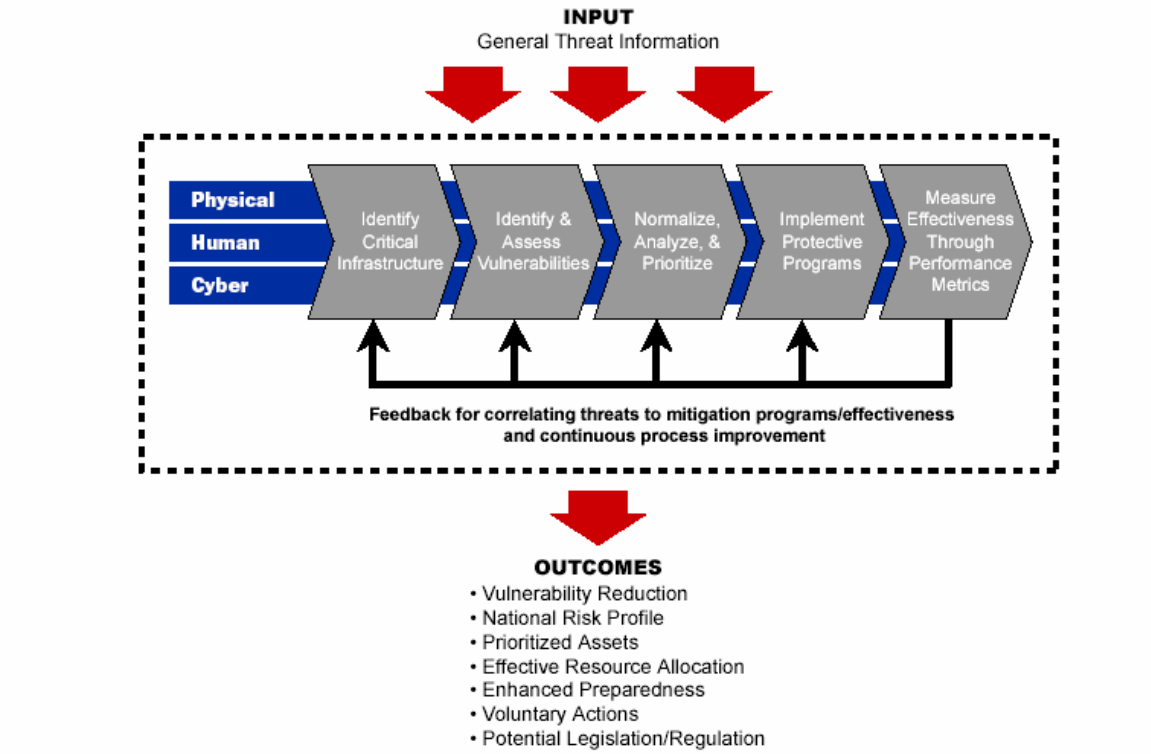
National Response Plan and National Incident Management System



Specific requirements in support of NRP and NIMS implementation have been placed on county, municipal, and state emergency management agencies and on local emergency response agencies, including law enforcement. Public transportation agencies now must address these requirements through greater integration in the local/regional/state emergency planning process and through adoption and implementation of NIMS.

To support implementation of **HSPD-7 (Critical Infrastructure Identification, Prioritization, and Protection)**, DHS issued the Interim National Infrastructure Protection Plan (NIPP) in February 2005. The NIPP provides a consistent, unifying structure for integrating critical infrastructure protection (CIP) efforts into a national program. The NIPP outlines how DHS and its stakeholders will develop and implement the national effort to protect infrastructures across all sectors, including transportation. DHS and the Sector-Specific Agencies (SSAs) are evaluating the Interim NIPP with critical stakeholders to further ensure its effectiveness and success. As depicted in the figure on the next page, DHS has developed a risk management framework to be used in evaluating vulnerabilities and establishing priorities in each of the 17 sectors identified as containing critical infrastructure or key resources. Public transportation is included as a critical infrastructure.

DHS Risk Management Process for Critical Infrastructure Protection



For public transportation, DHS has identified representative measures of efforts being made across the United States. These measures involve a layered approach to enhancing the safety and security of its transit systems. Some of the elements of this approach include:

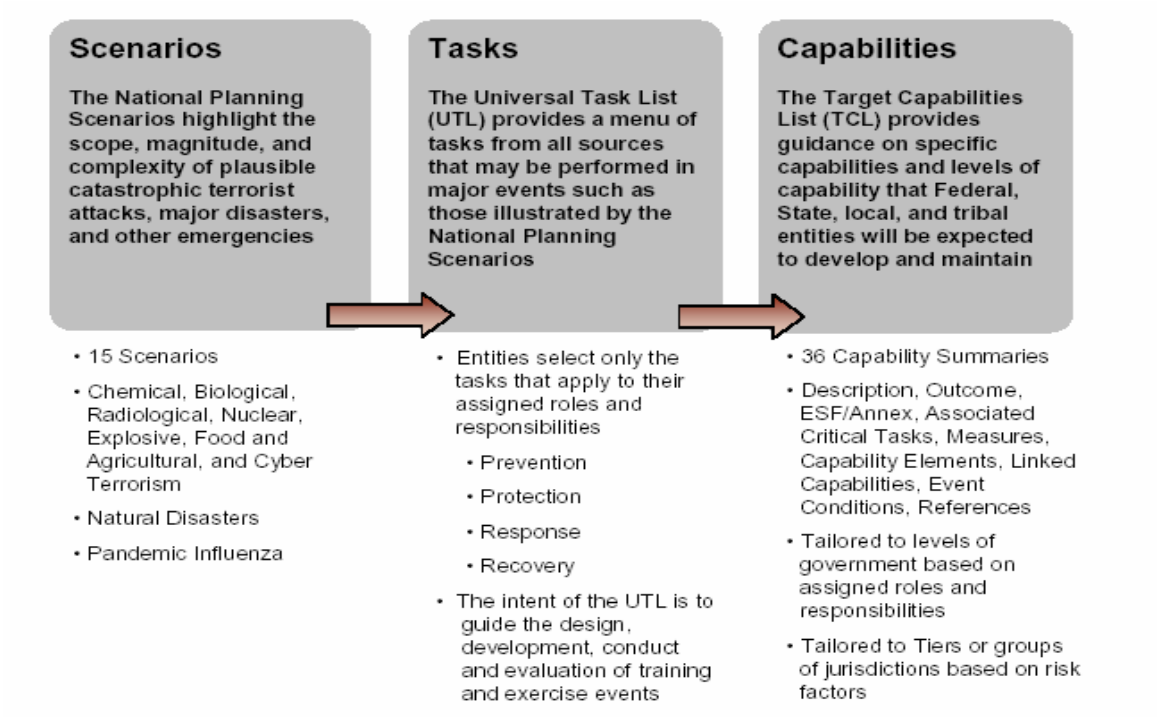
- the **increased presence of law enforcement** to deter potential terrorists and to possibly identify threats, as well as to provide additional first response capabilities should an event occur;
- the **selected deployment of sensors and other detection devices** to deter terrorists and to quickly identify the presence of various chemical, biological, radiological, nuclear, or explosive materials in order to minimize the consequences of an attack;
- the **application of facial recognition and other screening technologies** in order to identify suspect individuals;
- **training for employees and the traveling public** to increase awareness of suspicious individuals and packages and the need to promptly report them;
- **daily sharing of threat information and best practices** for protective measures across different transit systems;
- **development of emergency response and evacuation plans** to assist in rapid evacuations and control of any situations that occur;
- **development of recovery plans** to allow safe operations to resume as quickly as possible after a shutdown (with or without an actual attack);
- **selective closures** of entrances and exits where the service benefit is low and the security concerns are high;
- **greater separation** of passenger areas from those that are open to the public;

- **use of access control systems, badges and uniforms** to more readily identify employees and those that are supposed to be in restricted areas; and
- **greater cooperation and interaction** with local, state, and federal law enforcement and intelligence agencies to ensure that critical information is shared.

HSPD-8 (National Preparedness) establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters and other emergencies by requiring a National Preparedness Goal, establishing mechanisms for improved delivery of federal preparedness assistance to state and local governments and outlining actions to strengthen preparedness capabilities of federal, state, and local entities. Statewide all-hazards preparedness strategies should be consistent with the National Preparedness Goal, assess the most effective ways to enhance preparedness, address areas facing higher risk especially to terrorism, and address local government concerns and Citizen Corps efforts.

The National Preparedness Goal establishes the requirement for federal, state, local and tribal entities to achieve and sustain nationally accepted risk based target levels of capability for prevention, preparedness, response and recovery for major events, especially terrorism. The target levels of capability are based upon National Planning Scenarios, a Universal Task List (UTL), and a Target Capabilities List (TCL). These tools have been developed with input from the homeland security community at all levels and will continue to be updated over time. States should take steps in FY05 to review and incorporate these tools in their preparedness efforts in preparation for full implementation of HSPD-8 in FY06. The figure below provides a visual depiction of the interfaces among the National Planning Scenarios, the Universal Task list, and the Target Capabilities List.

Elements of the National Preparedness Goal



The 36 Critical Capabilities required to ensure National Preparedness are listed below:

Critical Capabilities

1. Animal Health Emergency Support
2. CBRNE Detection
3. Citizen Preparedness and Participation
4. Citizen Protection: Evacuation and/or In-Place Protection
5. Critical Infrastructure Protection
6. Critical Resource Logistics and Distribution
7. Economic and Community Recovery
8. Emergency Operations Center Management
9. Emergency Public Information and Warning
10. Environmental Health and Vector Control
11. Explosive Device Response Operations
12. Fatality Management
13. Firefighting Operations/Support
14. Food and Agriculture Safety and Defense
15. Information Collection and Threat Recognition
16. Information Sharing and Collaboration
17. Intelligence Fusion and Analysis
18. Interoperable Communications
19. Isolation and Quarantine
20. Mass Care (Sheltering, Feeding, and Related Services)
21. Mass Prophylaxis
22. Medical Supplies Management and Distribution
23. Medical Surge
24. On-Site Incident Management
25. Planning
26. Public Health Epidemiological Investigation and Laboratory Testing
27. Public Safety and Security Response
28. Restoration of Lifelines
29. Risk Analysis
30. Search and Rescue
31. Structural Damage Assessment and Mitigation
32. Terrorism Investigation and Intervention
33. Triage and Pre-Hospital Treatment
34. Volunteer Management and Donations
35. WMD/Hazardous Materials Response and Decontamination
36. Worker Health and Safety

For HSD-8, DHS has identified seven National Priorities, based on the scenarios, task list and critical capabilities, as building blocks for the National Preparedness System. These seven priorities reflect a limited number of the cross-cutting initiatives and critical capabilities that should drive near-term planning and resource allocation efforts. The National Priorities are intended to guide the nation's preparedness efforts to meet its most urgent needs, and fall into two categories: (1) overarching priorities that contribute to the development of multiple capabilities, and (2) capability-specific priorities that build selected capabilities for which the nation has the greatest need.

<u>Overarching Priorities</u>

1. Implement the National Incident Management System and National Response Plan
2. Expanded Regional Collaboration
3. Implement the Interim National Infrastructure Protection Plan

<u>Capability-Specific Priorities</u>

4. Strengthen Information Sharing and Collaboration capabilities
5. Strengthen Interoperable Communications capabilities
6. Strengthen CBRNE Detection, Response, and Decontamination capabilities
7. Strengthen Medical Surge and Mass Prophylaxis capabilities

IMPLICATIONS FOR THE RAIL TRANSIT AGENCY

HSPD-5: NRP: Requirements for the NRP are being addressed by the state Emergency Management Agency (EMA) in revising the state Emergency Operations Plan. The county EMA and/or a specially created County Advisory Board (CEM Board) and the major municipality served by the rail transit agency are also preparing Emergency Operations Plans for the county and city respectively, which reflect requirements from the NRP and the state EOP. The rail transit agency, in turn, is addressing these requirements through participation in the Major Emergency Incident Management System (MEIMS) established for the county/municipality and through the submission of its EOP to the appropriate municipal and county agencies. The rail transit agency is also revising its MOUs and response protocols with the municipality and county, and preparing an itemized inventory of emergency response resources.

The rail transit agency's cooperative agreement with the county EMA extends to mutual aid with participating communities. In addition, the county coordinate's homeland security related emergency management planning through the Urban Area Security Initiative (UASI) Point-of-Contact Committee (UAPOC).

HSPD-5: NIMS: To address NIMS requirements, the rail transit agency has developed and documented its **Incident Management Organization** and emergency notification and response procedures in its Emergency Operations Plan. The rail transit agency EOP:

- incorporates NIMS into emergency operations planning;
- incorporates NIMS into existing training programs and exercises;
- revises/updates mutual aid agreements with regional emergency management public safety agencies in the rail system's service area to address NIMS requirements; and,
- institutionalizes the rail transit agency's capabilities to interface with the Incident Command System (ICS) used by emergency management and public safety agencies in its service area.

The rail transit agency understands that full NIMS compliance is required for the receipt of preparedness grants from G&T and FEMA for FY 2007. FEMA's NIMS Integration Center (NIC) is continuing to develop resource materials and guidance (http://www.fema.gov/nims). In addressing NIMS requirements, the rail transit agency has committed to:

- Having relevant personnel complete the NIMS Awareness Course: "National Incident Management System (NIMS), An Introduction" IS 700. This independent study course is available on-line and will take between forty-five minutes to three hours to complete. The course is available on the Emergency Management Institute web page at: http://training.fema.gov/EMIWeb/IS/is700.asp.

- Formally recognizing NIMS and adopting NIMS principles and policies. The NIC will provide sample language and templates to assist in formally adopting NIMS through legislative and/or executive/administrative means.

- Establishing a NIMS baseline by determining which NIMS requirements are already satisfied. The NIC has developed a web-based self-assessment system, the NIMS

Capability Assessment Support Tool (NIMCAST) to evaluate their incident response and management capabilities. The NIC is currently piloting the NIMCAST with a limited number of states. Upon completion of the pilot, the NIC will provide all potential future users with voluntary access to the system. Additional information about the NIMCAST tool will be provided later this year.

- Establishing a timeframe and developing a strategy for full NIMS implementation. Rail transit systems are encouraged to achieve full NIMS implementation during FY 2005. To the extent that full implementation is not possible during FY 2005, federal preparedness assistance must be leveraged to complete NIMS implementation in FY 2006. By FY 2007, federal preparedness assistance will be conditioned upon full compliance with NIMS.

- Institutionalizing the use of the ICS. Transit systems that are not already using ICS, must institutionalize the use of ICS (consistent with the concepts and principles taught by DHS) across the entire response system.

The rail transit agency is also addressing NIMS requirements through its partnership with the county and municipal emergency management agencies in its service area. The county has approved the Major Emergency Incident Management System (MEIMS) Basic Principals and Protocols. *MEIMS Basic Principles* establish Emergency Incident Levels and define the roles and responsibilities of the various entities, including the rail transit agency, which could become involved in emergency response. *MEIMS Protocols*, which have been adopted by the rail transit agency, specify use of the Incident Command System (ICS) and support compliance with the National Incident Management System (NIMS) and the National Response Plan (NRP) regarding both on-scene response and the request and mobilization of resources.

HSPD-7: NIPP: In developing its Emergency Operations Plan, SEPP, and supporting procedures, plans, policies, training, drills/exercises, and other activities, the rail transit agency is addressing concerns identified in the NIPP. Further, the rail transit agency remains committed to filling requests from DHS or SSAs regarding:

- the identification and prioritization of assets;
- the sharing of data with DHS & SSAs and the response to all calls for such data;
- the verification and update of data based on knowledge, practice and observations;
- the conduct of shared assessments with DHS and SSAs;
- the identification of infrastructure interdependencies; and
- the development of cross-sectional prioritization efforts.

HSPD-8: G&T Transit Security Grant Program: G&T requires fulfillment of DHS emergency preparedness guidance as a condition of eligibility for security preparedness grants and technical assistance. G&T includes a Transportation Infrastructure Security Division (TISD) which administers the Urban Area Security Initiative (UASI), Transit Security Grant Program (TSGP). This program requires that the rail transit agency work with its State Administrative Agency (SAA), and the state Emergency Management Agency, to:

- Provide a point-of-contact and a program narrative describing the rail transit system, including a description of its operating systems, infrastructure, ridership, the number of

track miles (if applicable), the number of vehicles or vessels (if applicable), types of service and other important features, as well as system maps, a description of the geographical borders of the transit systems and the cities and counties served, and a description of other sources of funding being leveraged for security enhancements. In addition, the program narrative should address the rail transit agency's current prevention, detection and response capabilities relative to improvised explosive devices (IEDs), as well as chemical, biological, radiological and nuclear (CBRNE) devices, including sensors, canine units, etc.

- Ensure that the rail transit agency has conducted a transit threat and vulnerability assessment (either as outlined in *The Public Transportation System Security and Emergency Preparedness Planning Guide*, published by the U.S. Department of Transportation's Federal Transit Administration, January 2003 or through the Security Readiness Assessment conducted by the FTA, or through risk assessments that were completed during the previous round of UASI Transit Security Grants or the risk assessment completed as part of the G&T Mass Transit Technical Assistance Program). These assessments must be provided to G&T.

- Develop a Security and Emergency Preparedness Plan (SEPP), updated within the past year, which addresses the requirements outlined in *The Public Transportation System Security and Emergency Preparedness Planning Guide.* This plan must be provided to G&T for the release of TSGP funds.

- The program also includes a requirement that transit systems selected for funding participate in a Regional Transit Security Working Group (RTSWG) for the purpose of developing a Regional Transit Security Strategy (RTSS), and to develop regional consensus on the expenditure of FY 2005 TSGP funds. The RTSWG must also include representation from the state Emergency Management Agency and the state Department of Public Safety, Division of Homeland Security and the local Urban Area Working Group (UAWG). Other transit agencies whose systems intersect with the rail transit agency also participate in the RTSWG process.

  The focus of the regional transit system security strategy is on the detection of, response to, prevention of and recovery from terrorist incidents. First and foremost is the threat of improvised explosive devices and chemical, biological, radiological, nuclear, and explosive devices. This strategy will work hand in hand with existing regional, state homeland security, and urban area security initiative strategies, with particular emphasis on the transit system. A significant aspect of this strategy will be on the development of relationships, sharing of communications networks, tactical interoperable radio systems, shared technology, equipment, training and exercises.

- **Other Elements: Public Awareness and Citizen Participation:** Citizens are a critical component of homeland security, and to have a fully prepared community, citizens must be fully aware, trained, and practiced on how to detect, deter, prepare for, and respond to emergency situations. Recent surveys indicate that citizens are concerned about the threats facing the nation and are willing to participate to make their communities safer, yet most Americans have low awareness of federal, state, and local emergency preparedness plans, are not involved in local emergency drills, and are not adequately prepared at home.

Informed and engaged citizens are an essential component of homeland security and the mission of Citizen Corps is to have everyone in America participate in making their community safer, stronger, and better prepared. To achieve this, state, local and tribal Citizen Corps Councils have formed nationwide to help educate and train the public, and to develop citizen/volunteer resources to support local emergency responders, community safety, and disaster relief.

In support of this mission, G&T is currently working with FTA to align the Citizen Corps and Transit Watch programs. As part of this, all FY 2005 TSGP award recipients should work with the applicable state and local Citizen Corps Councils to more fully engage citizens through the following activities:

- Expand plans and task force memberships to address citizen participation.
- Develop or revise plans to integrate citizen/volunteer resources and participation, and include advocates for increased citizen participation in task forces and advisory councils.
- Awareness and outreach to inform and engage the public. Educate the public on personal preparedness measures, terrorism awareness, alert and warning systems, and state and local emergency plans via a range of community venues and communication channels.
- Include citizens in training and exercises. Provide emergency preparedness and response training for citizens, improve training for emergency responders to better address special needs populations, and involve citizens in all aspects of emergency preparedness exercises, including planning, implementation, and after action review.
- Develop or expand programs that integrate citizen/volunteer support for the emergency responder disciplines. Develop or expand Citizen Corps Programs into the transit environment, including citizen participation in prevention and response activities.

In addition, FY2005 TSGP award recipients should also take advantage of the public awareness materials developed by FTA through Transit Watch. To facilitate this, reproduction of official Transit Watch materials is an allowable expense as part of this program.

TSA REGULATIONS:

Under authority of 49 USC 40119, USDOT and TSA have jointly issued, at 49 CFR § 15 and 49 CFR § 1520 respectively, regulations for protection of sensitive security information (SSI), applicable to all modes of transportation. The rail transit agency uses its legal department to address SSI considerations, and, at the present time, does not need protections afforded by these regulations.

In addition, the Transportation Security Administration (TSA) has required, per its security directive RAILPAX-04-01 issued May 20, 2004, the designation of primary and alternate security coordinators (SCs) for public mass transit rail operations. The rail transit agency has provided these SCs to TSA.

The SCs serve as point-of-contact with TSA, such as rail security inspectors under TSA's Surface Transportation Security Inspector (STSI) program. Pursuant to the DHS/G&Ts National Infrastructure Protection Plan (NIPP) and DHS/TSA's Transportation Security Operational Plan (TSOP), TSA has developed a Surface Transportation Security Inspector (STSI) Program (Rail), as mandated by the Fiscal Year 2005 Homeland Security appropriations bill.

The STSI program will hire, train and deploy 100 TSA rail security compliance inspectors, to be located in 19 cities. The cities were chosen for their proximity to major rail hubs, existing Federal Railroad Administration (FRA) and Federal Transit Administration offices, and existing TSA Aviation Operations Districts. In coordination with mass transit and passenger rail systems, the TSA inspectors will: conduct security system evaluations; share security-related best practices information; coordinate security threat advisories; and conduct inspections to ensure compliance with security directives, such as TSA's security directive RAILPAX-04-01 issued May 20, 2004.

Appendix B: Acronyms

AVL	Automatic Vehicle Location
BASS	Behavioral Awareness Security Screening
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive (WMD)
CCTV	Closed-Circuit Television
COOP	Continuity of Operations Plan
CFR	Code of Federal Regulations
CPTED	Crime Prevention Through Environmental Design
DHS U.S.	Department of Homeland Security
DOT U.S.	Department of Transportation
EMS	Emergency Medical Services
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
G&T	Office of Grants and Training
HSPD	Homeland Security Presidential Directive
IED	Improvised Explosive Device
JTTF	Joint Terrorism Task Force (FBI)
NIMS	National Incident Management System
NTI	National Transit Institute
OCC	Operations Control Center
ODP	Office for Domestic Preparedness
OSHA	Occupational Safety and Health Administration
POETE	Plans, Organization, Equipment, Training/Procedures, and Exercises/Evaluation
RFGS	Rail Fixed Guideway System
RTSS	Regional Transit Security Strategy
SEPP	Security and Emergency Preparedness Plan
SOP	Standard Operating Procedure
SSO	RFGS State Safety Oversight Agency
SSPP	System Safety Program Plan
TEW	Terrorism Early-Warning System
TSA	Transportation Security Administration
UA	Urban Area (for DHS/G&T administration of UASI program)
UAPOC	Regional UASI Point-of-Contact working group
UASI	Urban Areas Security Initiative
WMD	Weapons of Mass Destruction

Appendix C: Definitions

Assessment - The evaluation and interpretation of measurements and other information to provide a basis for decision-making.

Assets - People, information, and property for which the public transportation system is responsible as legal owner, employer, or service provider.

Capabilities Assessment - A formal evaluation, conducted by the public transportation system, to identify the status of its security and emergency preparedness activities. This activity enables the system to determine its existing capacity to: (1) Reduce the threat of crime and other intentional acts, (2) Recognize, mitigate, and resolve incidents that occur in service and on system property, (3) Protect passengers, employees, emergency responders, and the environment during emergency operations, and (4) Support community response to a major event.

Consequences - The severity of impact and probability of loss for a given threat scenario. Consequences may be measured in qualitative or quantitative terms.

Countermeasures - Those activities taken to reduce the likelihood that a specific threat will result in harm. Countermeasures typically include the deployment and training of personnel, the implementation of procedures, the design or retrofit of facilities and vehicles; the use of specialized equipment, the installation of alarms/warning devices and supporting monitoring systems; and communications systems and protocols.

Critical Assets - A sub-category of assets whose loss has the greatest consequences for people and the ability of the system to sustain service. These assets may require higher or special protection.

Critical Infrastructure - Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (USA Patriot Act of 2001, 42 U.S.C. § 5195(e), incorporated by reference into the Homeland Security Act of 2002, 6 U.S.C. § 101).

Department of Homeland Security (DHS) - U.S. government agency created by the Homeland Security Act of 2002 (Pub. L. 107-296). Includes Transportation Security Administration (TSA), and within the Office of the Secretary of DHS, the Office for Domestic Preparedness (ODP), which is now referred to as the Department of Homeland Security, Preparedness Directorate, Office of Grants and Training (G&T). TSA's authority includes regulation and oversight of security measures for all modes of transportation in the United States. G&T's functions include coordinating emergency preparedness efforts at all levels of government.

Emergency - A condition, situation or occurrence of a serious nature, developing suddenly and unexpectedly, and requiring immediate action.

Emergency Operations Center (EOC) - The physical location at which the coordination of information and resources to support domestic incident management activities normally takes place.

Emergency Operations Plan (EOP) - The formal plan that documents the transportation system's program for emergency preparedness and response.

Emergency Preparedness - Plans, organization, equipment, training/procedures, and exercises/evaluation, for preparedness to perform the prevention, detection, response and recovery capabilities applicable to mass transit employees and operations during catastrophic natural disasters, or terrorist attacks, appropriately coordinated/integrated with emergency response/management jurisdictions in the transit agency's service area.

Emergency Responder - Federal, state, and local public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities.

Evacuation - Organized, phased, and supervised withdrawal, dispersal, or removal of civilians from dangerous or potentially dangerous areas, and their reception and care in safe areas.

Event - A planned, non-emergency activity. ICS can be used as the management system for a wide range of events, e.g., parades, concerts, or sporting events.

Federal Transit Administration (FTA) - The agency of the U.S. Department of Transportation which administers the federal program of financial assistance to public transit.

Hazard also Hazardous Condition - Any real or potential condition that can cause injury, illness, or death; damage to or loss of a system, equipment or property; or damage to the environment.

Hazard Severity -

Catastrophic - A hazard severity category defined as "Category I" failure condition that could result in a large number of serious injuries and/or fatalities, and/or significant loss of system capability.

Critical - A hazard severity category defined as "Category II" failure condition that could result in severe injury to one or more persons, and/or significant system damage.

Marginal - A hazard severity category defined as "Category III", failure conditions that could result in minor injury, minor occupational illness, or minor system damage.

Negligible - A hazard severity category defined as "Category IV" failure conditions that cause less than minor injuries, illness, or system damage.

Hazard Threat Probability – The probability a hazard or threat will occur. Probability may be expressed in quantitative or qualitative terms and the ranking system is as follows: (a) frequent, (b) probable, (c) occasional, (d) remote, (e) improbable, and (f) impossible.

Hazard Resolution – The analysis and subsequent actions taken to reduce, to the lowest level practical, the risk associated with an identified hazard.

Homeland Security Presidential Directives (HSPDs) - instruments for communicating presidential decisions about the national security policies of the United States and implementations thereof.

Incident – An occurrence or event, natural or human-caused, which requires an emergency response to protect life or property.

Incident Command System (ICS) - A standardized on-scene emergency management concept specifically designed to provide for the adoption of an integrated organizational structure that reflects the complexity and demands of single or multiple incidents, without being hindered by jurisdictional boundaries. ICS is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents.

Incident Commander (IC) - The individual responsible for all incident activities, including the development of strategies and tactics and the ordering and the release of resources. The IC has overall authority and responsibility for conducting incident operations and is responsible for the management of all incident operations at the incident site.

Injury – Injury to a person requiring medical attention necessitating transport to a medical facility by ambulance or police vehicle for medical treatment.

Investigation - The process used to determine the causal and contributing factors of an accident or hazard, so that actions can be identified to prevent recurrence.

Management Loss Control - An element of the system safety and security management function that evaluates the effects of potential hazards/threats considering acceptance, control, or elimination with respect to the expenditure of available resources.

Mitigation - The activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident. Mitigation measures may be implemented prior to, during, or after an incident. Mitigation measures are often informed by lessons learned from prior incidents. Mitigation involves ongoing actions to reduce exposure to, probability of, or potential loss from hazards.

Multi-jurisdictional Incident - An incident requiring action from multiple agencies that each have jurisdiction to manage certain aspects of an incident. In ICS, these incidents will be managed under Unified Command.

Mutual-Aid Agreement - Written agreement between agencies and/or jurisdictions that they will assist one another on request, by furnishing personnel, equipment, and/or expertise in a specified manner.

National Incident Management System - A system mandated by HSPD-5 pursuant to the Homeland Security Act of 2002, that provides a consistent nationwide approach for federal, state, local, and tribal governments; the private-sector, and nongovernmental organizations to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among federal, state, local, and tribal capabilities, the NIMS includes a core set of concepts, principles, and terminology. HSPD-5 identifies these as the ICS; multi-agency coordination systems; training; identification and management of resources (including systems for classifying types of resources); qualification and certification; and the collection, tracking, and reporting of incident information and incident resources.

National Infrastructure Protection Plan (NIPP): A DHS/TSA-issued plan, mandated by HSPD-7 pursuant to the Homeland Security Act of 2002, for protection of critical infrastructure in the United States. The plan designates TSA as the sector-specific federal agency responsible for transportation critical infrastructure protection. In 2005, TSA is developing a Transportation Security Operational Plan (TSOP) that (1) will describe responsibilities and program milestones for securing critical transportation infrastructure in areas of domain awareness, prevention, protection, response, and recovery; and (2) will provide transportation owner/operators with guidance to develop or enhance their respective security plans.

National Response Plan - A DHS/G&T-issued plan, mandated by HSPD-5 pursuant to the Homeland Security Act of 2002, that integrates federal domestic prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan.

National Preparedness Goal and National Preparedness Plan - A DHS/G&T-issued plan, mandated by HSPD-8 pursuant to the Homeland Security Act of 2002, that provides a consistent nationwide approach and objectives for federal, state, local, and tribal governments to develop plans, organization, equipment, training/procedures, and exercises/evaluation, for preparedness to perform the prevention, detection, response and recovery capabilities (as specified in the DHS/G&T-issued Target Capabilities List) during catastrophic natural disasters or terrorist attacks (particularly as specified in the DHS/G&T-issued National Planning Scenarios).

Office of Domestic Preparedness (ODP) - see Department of Homeland Security (DHS)

Office of Grants and Training (G&T) – see Department of Homeland Security (DHS)

Off-Peak Period - The period between the morning and evening peak periods when travel activity is generally lower and less transit service is scheduled.

Park and Ride Lot - Designated parking areas for automobile drivers who then board transit vehicles from these locations.

Peak Period - Morning and afternoon time periods when transit riding is heaviest.

Preparedness - The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents.

Prevention - Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice.

Procedures - Established and documented methods to perform a series of tasks.

Public Information Officer - A member of ICS Command Staff responsible for interfacing with the public and media or with other agencies with incident-related information requirements.

Public Transit System - An organization that provides transportation services owned, operated, or subsidized by any municipality, county, regional authority, state, or other governmental agency, including those operated or managed by a private management firm under contract to the government agency owner.

Recovery - The development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private sector, nongovernmental, and public-assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents.

Response - Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and of mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into the nature and source of the threat; on-going public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at

preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Redundancy - The existence of more than one means of accomplishing a given function.

Ridership - The number of rides taken by people using a public transportation system in a given time period.

Risk Assessment –

Initial Risk Index - The index of the worst credible consequences resulting from the hazard.

Residual Risk Index - The index of the worst credible consequences resulting from the hazard once corrective actions have been implemented.

Safety - Freedom from harm resulting from unintentional acts or circumstances.

Safety Certification - An element of the System Safety Program that documents the functional working of the System Safety Program, and provides a documented database from which to validate the active processes necessary to produce a safe system, ready for revenue service. Used primarily on new systems and expansions of operational properties.

Scenario Analysis - An interpretive methodology that encourages role-playing by transportation personnel, emergency responders, and contractors to brainstorm ways to attack the system. This analysis uses the results of threat analysis, paired with the system's list of critical assets. Transportation personnel use this analysis to identify the capabilities required to support specific types of attacks. This activity promotes awareness and highlights those activities that can be preformed to recognize, prevent, and mitigate the consequences of attacks.

Security - Freedom from harm resulting from intentional acts or circumstances.

Security Breach - An unforeseen event or occurrence which endangers life or property and may result in the loss of services or system equipment.

Security Threat - Any intentional action with the potential to cause harm in the form of death, injury, destruction, disclosure, interruption of operations, or denial of services.

Sensitive Security Information (SSI) - Information as described at 49 CFR § 1520.5 / 49 CFR § 15.5. SSI is information obtained or developed in the conduct of security activities, the disclosure of which would be detrimental to transportation safety. SSI includes: security program plans, security and vulnerability assessments, threat information, incident response plans, security directives and measures, security inspection or investigative information, security screening information or procedures, specifications for devices for detection of weapons or destructive devices or substances, specifications for communications equipment used for transportation security, and critical infrastructure information (see Critical Infrastructure).

System - A composite of people (employees, passengers, others), property (facilities and equipment), environment (physical, social, institutional), and procedures (standard operating, emergency operating, and training) which are integrated to perform a specific operational function in a specific environment.

System Security - The application of operating, technical, and management techniques and principles to the security aspects of a system throughout its life to reduce threats and vulnerabilities to the most practical level through the most effective use of available resources. System Security Program is the combined tasks and activities of system security management and system security analysis that enhance operational effectiveness by satisfying the security requirements in a timely and cost-effective manner through all phases of a system life cycle. System Security Management is an element of management that defines the system security requirements and ensures the planning, implementation, and accomplishments of system security tasks and activities.

System Security Program Plan - a document developed and adopted by a transit agency describing its security policies, objectives, responsibilities, and procedures.

Terrorism - Under the Homeland Security Act of 2002, terrorism is activity that involves an act dangerous to human life or potentially destructive of critical infrastructure or key resources and is a violation of the criminal laws of the United States or of any state or other subdivision of the United States in which it occurs and is intended to intimidate or coerce the civilian population or influence a government or affect the conduct of a government by mass destruction, assassination, or kidnapping.

Threat - An indication of possible violence, harm, or danger. Any real or potential condition that can cause injury or death to passengers or employees of damage to or loss of transit equipment, property, and/or facilities.

Threat and Vulnerability Assessment: An evaluation performed to consider the likelihood that a specific threat will endanger the system, and to prepare recommendations for the elimination or mitigation of all threats with attendant vulnerabilities that meet pre-determined thresholds. Critical elements of these assessments include:

Threat Analysis - Defines the level or degree of the threats against a specific facility by evaluating the intent, motivation, and possible tactics of those who may carry them out.

Threat Probability - The probability a threat will occur at a specific facility during its life cycle (typically quantified as 25 years), for example:

Frequent: Event will occur within the system's lifecycle.
Probable: Expect event to occur within the system's lifecycle.
Occasional: Circumstances expected for that event; it may or may not occur within the system's lifecycle.
Remote: Possible but unlikely to occur within the system's lifecycle.
Improbable: Event will not occur within the system's lifecycle.

Threat Severity - A qualitative measure of the worst possible consequences of a specific threat in a specific facility:

Category 1 - Catastrophic: May cause death or loss of a significant component of the transit system, or significant financial loss.

Category 2 - Critical: May cause severe injury, severe illness, major transit system damage, or major financial loss.

Category 3 - Marginal: May cause minor injury or transit system damage, or financial loss.

Category 4 - Negligible: Will not result in injury, system damage, or financial loss.

Threat Resolution - The analysis and subsequent action taken to reduce the risks associated with an identified threat to the lowest practical level.

Transportation Security Administration (TSA) - see Department of Homeland Security (DHS).

Unified Command - An application of ICS used when there is more than one agency with incident jurisdiction or when incidents cross political jurisdictions. Agencies work together through the designated members of the UC, often the senior person from agencies and/or disciplines participating in the UC, to establish a common set of objectives and strategies and a single IAP.

Unsafe Condition or Act - Any condition or act which endangers life or property.

Urban Area Security Initiative (UASI) - A security grant assistance program of the U.S. Department of Homeland Security (DHS), administered through the Office of Grants and Training. UASI provides grant assistance to address the unique planning equipment training and exercise needs of identified high-risk urban areas (UAs), ports and mass transit agencies, and to assist them in building an enhanced capability to prevent, respond to, and recover from acts of terrorism.

Vulnerability - Characteristics of passengers, employees, vehicles, and/or facilities which increase the probability of a security breach.

Vulnerability Analysis: The systematic identification of physical, operational and structural components within transportation facilities and vehicles that can be taken advantage of to carry out a threat. This includes vulnerabilities in the design and construction of a given transit facility or vehicle, in its technological systems, and in the way it is operated (e.g., security procedures and practices or administrative and management controls). Vulnerability analysis identifies specific weaknesses with respect to how they may invite and permit a threat to be accomplished.